

**Wireless Local
Area
Network (WLAN)
Best Practices
Guide**

**Prepared by
Stakeholder Technology
Branch**

October 2007



Alberta

Wireless Local Area Network (WLAN) Best Practices Guide

This document is available on the Internet at:

<http://www.int.ca>

Copyright © 2007 Crown in Right of the Province of Alberta, as represented by the Minister of Education.

Permission is hereby given by the copyright holder to use, reproduce, store or transmit this material for educational purposes and on a non-profit basis. However, Crown copyright is to be acknowledged. If this material is to be used, reproduced, stored or transmitted for commercial purposes, arrange first for consent by contacting:

Stakeholder Technology Branch

Alberta Education

10th Floor, 44 Capital Boulevard

10044-108 Street Edmonton, AB T5J 5E6

Telephone: (780) 427-9001 (toll-free in Alberta by dialing 310-0000 first)

Fax: (780) 415-1091

ALBERTA EDUCATION CATALOGUING IN PUBLICATION DATA

Alberta. Alberta Education. Stakeholder Technology branch.

Wireless local area network (WLAN) best practices guide.

ISBN 978-0-7785-6411-9

1. Wireless LANs -- Handbooks, manuals, etc. 2. Wireless LANs -- Security measures -- Handbooks, manuals, etc. 3. Computer networks. I. Title.

TK5105.78 A333 2007

004.68

Table of Contents

Chapter 1 Introduction	5
1.1 Alberta's Education System and Wireless LANs	6
Audience	6
Sources	6
Scope	6
How to Read and Use this Document	7
Chapter 2 Wireless Technology Overview	8
2.1 Overview of Wireless Technology	9
LANs, WLANs and Protocols	9
Standards for Communication: The 802.11 Specification	9
How WLANs Communicate	12
Channels	14
2.2 Wireless Security Standards	19
EAP and 802.1X Authentication Protocols	19
WLAN Authentication and Encryption	21
Virtual Private Network (VPN)	25
2.3 Overview of Wireless Market and Vendors	27
Market Overview	27
Market Description	28
Vendors	29
Chapter 3 Going Wireless Preparation and Planning	30
3.1 First Steps	31
Setting Realistic Goals and Expectations	31
Team, Roles and Responsibilities	32
Specific one-to-one Initiative Considerations	32
3.2 Analysis	32
Immediate Scope and Future Scalability	32
Budget Requirements and Limitations	33
Technology Selection	33
3.3 Project Plan	41
Timeframe	41
Scope	42
3.4 Technical Deployment Considerations	45
Network	45
Alberta SuperNet	47
Site Survey	47
Signal Strength	49
Impact of Device Standards, Ownership and Mobility	57
School and/or Home Usage	58
Integration of Student Owned Devices	58
Chapter 4 Security	59
4.1 Security Policy	60
4.2 Network Security	62
Network Based Firewalls and Traffic Topology	62
Virtual Private Networks (VPN) and Proxy Servers	63
Intrusion Detection and Prevention (IDS/IDP)	64
Virtual Local Area Networks (VLANs)	64

4.3	Wireless Security	65
	Avoiding Common Wireless Security Oversights	65
	Network Access Control (NAC)	66
	Guest Access	67
4.4	Mobile Host Security	68
	Security Software and Operating System Updates	68
	Personal Firewalls	68
	Anti-Virus (A/V)	68
	Anti-Spyware (A/S)	69
	Encrypted File Systems (EFS)	69
4.5	Content Security	70
Chapter 5	Making the Best Decision for your School(s)	71
	One-to-One Initiatives Today and Tomorrow	72
Chapter 6	Implementation	74
	Checklist	75
	Communication	76
	Piloting and Roll-Out	76
	Documentation	76
	Trouble Shooting Tips	77
	WLAN Performance Testing and Tuning	77
Chapter 7	Case Studies	778
7.1	Introduction	79
7.2	Calgary Board of Education (CBE)	80
7.3	Calgary Catholic School District (CCSD)	83
7.4	Evergreen Catholic School District (ECSD)	85
	Glossary Terms and Acronym Key	87
	Resources and Sources	89
	Links	89



Canada geese in flight © Chip Kelsey - fotolia.com

This chapter will cover:

- Alberta's Education System and Wireless LANs
- Audience
- Sources
- Scope
- Goals of this Document
- How to Read and Use this Document
- Contact Information
 - Vendors
 - Alberta Education
 - Southern Alberta Institute of Technology
 - Network Integrators of Canada Inc.

1.1 Alberta's Education System and Wireless LANs

WLANs (Wireless Local Area Networks) are playing an important role in Kindergarten to Grade 12 schools across Alberta by improving the value that IT brings to education. As with any technology, WLANs present some unique challenges. However, the combination of wireless technology's relatively low cost and easy deployment has led many districts implementing wireless technology without adequate up front planning and without addressing ongoing support requirements. This can lead to degraded levels of service and significant security exposures, dramatically increasing failure rates of user adoption and seamless usage.

Districts contemplating WLANs must address their network security and ongoing management practices, including associated tools, to adequately protect information security and provide reliable service. The ability to deliver quality education using WLAN technology will be improved by delivering consistent and reliable service.

Audience

The primary audience for this guide is IT directors and network personnel who are responsible for deploying and managing wireless related infrastructure in Alberta schools and supporting laptops and mobile devices in the classroom. This guide is not meant for educational coordinators or teachers. All levels of IT staff at both the district and local school level can benefit from information included in this guide.

Whether your district has already deployed some or even all of your schools with WLAN technology, or if you are just getting started, this guide will provide insight to all aspects of using wireless at your schools.

Sources

This guide was produced by The Southern Alberta Institute of Technology (SAIT) and Network Integrators of Canada (NI Canada) in conjunction with Alberta Education.

Many resources have been included from an array of global leading manufacturers of wireless hardware, software and related technology solutions. Refer to the section marked Resources and Sources for a detailed list of helpful reference materials and websites.

Scope

This guide is focused on WLANs and associated wireless technology. When addressing key aspects of technology such as WLANs, a comprehensive and holistic approach is required in order to truly derive an overall understanding of the complex, integrated and inter-dependent aspects of IT. Hence, further to wireless technology, the guide also delves into security issues. This area should be further addressed in order to gain a comprehensive understanding and view of wireless technology's role within your district's overall IT strategy.

How to Read and Use this Document

This document was created as a technical guide to assist K-12 school jurisdictions in implementing WLANs. The guide may be read front to back, cover to cover, and/or used as a reference for all aspects of the selection, configuration, security and ongoing management of WLANs.

This guide will walk you through the standards and protocols associated with wireless technology, the current market and some vendors, security strategies specific to wireless networks and to networks in general. Implementing solutions into your schools and information key to the ongoing management of your technology will also be addressed

For easy reference each chapter contains **Tips and Recommendations** listed in **graphical text boxes** like the one below within their associated section.

Tips will be included throughout various sections of the Guide and appear in a graphic text box like this one on the corresponding page.

Vendors of WLAN Solutions Include:

Table 1 - Vendor Websites

Vendor	Website Address
3Com	www.3com.com
Alcatel-Lucent	www.alcatel-lucent.com
Aruba Networks	www.arubanetworks.com
Bluesocket	www.bluesocket.com
Cisco Systems	www.cisco.com
Colubris	www.colubris.com
Enterasys Networks	www.enterasys.com
Extricom	www.extricom.com
Extreme Networks	www.extremenetworks.com
Foundry Networks	www.foundrynet.com
Hewlett-Packard	www.hp.com
Meru Networks	www.merunetworks.com
Nortel Networks	www.nortel.com
Siemens	www.siemens.com
Symbol Technologies / Motorola	www.symbol.com
Trapeze Networks	www.trapezenetworks.com
Vernier	www.vernier.com
Xirrus	www.xirrus.com



© Jaimie Duplass - Fotolia.com

- Overview of Wireless Technology
 - LANs, WANs and Protocols
 - Standards for Communication: The 802.11 Specification
 - How WLANs Communicate
 - Channels
- Wireless Security Standards
 - EAP and 802.11X Authentication Protocols
 - WLAN Authentication and Encryption
 - Virtual Private Network (VPN)
- Overview of Wireless Market and Vendors
 - Market Overview
 - Vendors

Chapter 2 Wireless Technology Overview

Wireless LANs are everywhere – at the office, at home, in the hotel, in the coffee shop or at the airport. The wireless concept that we take for granted now has its roots in the wireless modem of the early 90's. Early wireless modems were designed for single peripheral devices that needed a way to allow devices to send and receive computer data. The modem speeds that we had grown accustomed to were more than adequate for the task. Industry professionals drawn to this new emerging field are typically from the Information Systems Networking field with a strong background in the concepts of wired LAN, MAN and WAN or from the Radio Telecommunications field with an in-depth experience in wireless communication. This Wireless LAN field requires some degree of expertise in both. The hardware is typically added to an existing system as an extension of the Access Layer requirements of the network and managing the Air Interface requires another set of skills entirely. One of the best things about WLANs is that they operate in a license-free band allowing the market to develop products and technologies through open competition. One of the drawbacks with WLANs is that they operate in unlicensed bands, which results in increasing radio interference from other devices such as cordless phones. Industry Canada determines the frequency bands that WLANs operate in and the Institute of Electrical and Electronics Engineers (IEEE) develops the standards that describe how the technology will work in that spectrum.

2.1 Overview of Wireless Technology

LANs, WLANs and Protocols

What Is Wi-Fi?

Wi-Fi stands for Wireless Fidelity. Computers can be equipped with Wi-Fi adapters (which are available as internally-mounted cards, cards that fit in lap-top PCMCIA slots, or external devices attached via USB ports). Wi-Fi adapters are fairly inexpensive. The adapters seek out signals broadcast by devices called Access Points (APs) that in turn are typically connected to the existing wired network. This gives Wi-Fi devices access to the same resources that devices connected to the wired network have. Although it is less common, Wi-Fi devices can also communicate directly (one-to-one) with each other. Wi-Fi devices employ several different technical standards grouped together and referred to as the IEEE 802.11 specification in order to communicate with an AP.

What is the IEEE?

The IEEE (The Institute of Electrical and Electronics Engineers) creates and finalizes standards for computer networks, amongst other technologies. The IEEE 802.11 specification defines how wireless networks communicate. As a comparison, most wired networks based on Ethernet and CSMA/CD (defined later) technology conform to the 802.3 standard.

The Wi-Fi Alliance, to which all enterprise product manufacturers belong, guides the development of standards through product testing.

For more information, visit www.ieee.org.

Standards for Communication: The 802.11 Specification

802.11

In 1997 the IEEE published the original 802.11 – 1997 Std. In the industry it is often referred to as 802.11 prime as it was the initial wireless standard. It was revised in 1999 and reaffirmed in 2003 as 802.11 – 1999 (R2003). By this final reaffirmation most of the following subsets of the standard have their own section devoted to the idiosyncrasies of each. The original standard allowed for data rates at 1 or 2 Mbps. It contained three clauses defining physical layers. In Clause 16 it defined an Infrared (IR) physical layer which in the 802.11 form is obsolete. Clause 14 defined a Frequency Hopping Spread Spectrum (FHSS) physical layer; this technology has its roots as far back as WWII with the first known patent of its type. Clause 15 devices are defined as Direct Sequence Spread Spectrum (DSSS) and are the root of the subsequent amendments of 802.11a/b/g radio

devices. The Clause 16 or infrared devices are not considered a Radio Frequency technology, and due to their obsolete nature, will not be considered in this document.

All of the clause 14 and 15 devices or FHSS and DSSS devices operate in the 2.4 GHz Industrial, Scientific and Medical (ISM) Band as defined by Industry Canada. In Canada the IEEE restricts the operation of these devices to the Spectrum between 2.40 GHz and 2.4835 GHz. Clause 14 or FHSS devices are further restricted to 1 MHz wide carriers in the space between 2.402 GHz and 2.480 GHz, allowing a range of 78 individual carriers that can be organized into a pattern for the connected transmitter and receiver to follow in order to communicate. These FHSS radio devices cannot communicate with the DSSS radio devices. As manufacturers decided where to spend their research and development capital the DSSS radio devices and their apparent capabilities caused many of the major vendors to focus on the future and development of the DSSS or Clause 15 devices. The amendments of 802.11b and g were evidence of this as they both are backward compatible with the Clause 15 DSSS 802.11 prime devices but cannot communicate with the 802.11 Clause 14 FHSS devices.

802.11b

In 1999, 802.11b – 1999 was released and was later amended into the 802.11 standard. It defines operation in the 2.4 GHz radio band and DSSS only. The capabilities of adding two additional data rates of 5.5 Mbps and 11.0 Mbps created an even greater separation of demand for what was available at that time. This now gave DSSS a clear advantage over the legacy FHSS devices with their 2.0 Mbps maximum data rate. These new data rates are defined as High Rate DSSS (HR-DSSS).

802.11a

A second IEEE task group finished its project during 1999, which was ratified as 802.11a – 1999. Their mandate had been to define technologies that could operate in the newly available Unlicensed National Information Infrastructure (UNII) band. This use of Spread Spectrum was called Orthogonal Frequency Division Multiplexing (OFDM). This was initially defined as 3 - 100 MHz wide bands in the 5.8 GHz range. They are more commonly known as **UNII-Low** 5.150 – 5.250 GHz, **UNII-Mid** 5.250 – 5.350 GHz, and **UNII-Upper** 5.725 – 5.825 GHz. The lack of spectrum in the 2.4 GHz band required some additional spectrum allocation for Wireless Networks. More recently, a fourth band in the 5.8 GHz range was released and is known as the **UNII-New** 5.47 – 5.725 GHz band. The 802.11a devices are classed as Clause 17 devices in the 802.11 – 1999 (R2003) version of the standard. These 802.11a devices are not compatible with any of the other 802.11 technologies as they operate in a separate portion of the Radio Spectrum. At the time of release, their data rates of 6/9/12/18/24/36/48 and 54 Mbps were also incompatible with the 802.11 prime and 802.11b data rates. There are many multi-band cards available today that can support all 802.11a/b/g technologies.

802.11b/g

One amendment that was highly anticipated was the 802.11g – 2003 Std. These devices, defined as Clause 18 devices, operate in the 2.4 GHz spectrum, are compatible with the 802.11b legacy devices and capable of additional bandwidth. This standard combined the OFDM process of 6/9/12/18/24/36/48 and 54 Mbps data rates in addition to the backward compatibility to the data rates of 802.11b. It is described as Extended Rate Physical OFDM (ERP-OFDM). For the infrastructure device with this capability, it can be typically configured as one of the following: 802.11b only, 802.11g only or 802.11bg. This will have an impact on the effective throughput of the infrastructure device.

802.11g

When an 802.11b/g device is operating in the 802.11g mode, it operates as defined by Clause 19 of the standard and operates in the Orthogonal Frequency Division Multiplexing (OFDM) mode. This may also be referred to as a pure "G" system. In this mode of operation, it will not communicate with or allow 802.11b clients to participate on the network. In systems that are migrating from a completely 802.11b network, this would be the eventual goal.

802.11n

This IEEE task group has not yet ratified or released the 802.11n standard. Current equipment being marketed as "pre-n" may or may not be compatible with the official standard once it is released. The majority of this equipment

is being produced by the vendors for the SOHO wireless products as opposed to the enterprise models. As of March 12, 2007, the task group has approved Draft 2 of the standard which indicates that what remains to be completed is primarily the correction of the documentation before its sponsorship and ratification. Draft 2 is what will be used in technical aspects such as interoperability testing by the Wi-Fi alliance. The maximum data rate for 802.11n is to be 540 Mbps and this technology can be used in the 2.4 GHz as well as the 5.8 GHz frequency bands. Its range is predicted to be 50% greater than either 802.11a/b or g. With it still being about a year away from ratification and release to the general public, some questions still remain regarding what the adoption rate of this technology will be. We should see some Draft 2 products released prior to the end of this year.

802.11i

The IEEE 802.11i standard focuses on addressing all aspects of wireless security—even beyond client authentication and data privacy using WEP keys. As the 802.11i standard was being developed, wireless LAN vendors have moved ahead to implement as many of its features as possible. As a result, the Wi-Fi Alliance developed *Wi-Fi Protected Access (WPA)* based on some of the 802.11 draft components.

This is the most recent version of encryption for wireless networks. It is defined as MAC Layer Security Enhancements for 802.11. It increases the encryption sophistication of WEP using the Advanced Encryption Standard (AES). The hardware of devices that use 802.11i must be designed to handle AES. The two are not compatible, they are completely unique. Older legacy 802.11 products are not upgradeable. For some administrators, this provides some issues if they are upgrading their entire system to an 802.11i based encryption. Some of the equipment may simply need to be replaced in order to comply.

Comparison

Here is a comparison of the 802.11 standards. Note that 802.11n is not yet ratified:

Table 2 - 802.11 Speed Comparison

IEEE Wireless Specification Designation	Release Date	Operating Frequency Range	Throughput Speeds (maximum)	Effective Throughput Speeds* (typical)	Range (typical indoor distance in meters)*
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	54 Mbps	23 Mbps	~25 meters
802.11b	1999	2.4-2.5 GHz	11 Mbps	5 Mbps	~35 meters
802.11g	2003	2.4-2.5 GHz	54 Mbps	23 Mbps	~25+ meters
802.11n	2007 (unapproved draft)	2.4 GHz or 5 GHz bands	540 Mbps	100 Mbps	~50 meters

*Note that Speed and Ranges can vary dramatically based on environmental factors.

The effective throughput is limited by the half-duplex nature of this wireless technology, as well as the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA described below) mechanism which governs the use of the channel. This throughput could be achieved by a single client device using a particular Network Access Point all by itself. The available bandwidth must be shared between all clients connected to a particular Network Access Point.

The typical 802.11g device is also capable of 802.11b data rates, making the advertised range of all devices in the 2.4 GHz range the same. It is important to note that the advertised range is at the lowest data rate. 802.11a for example has 75 meters of range at 6 Mbps.

How WLANs Communicate

As a client brings up its wireless connection, it must find an Access Point (AP) that is reachable and that will approve its membership. The client must negotiate its membership and security measures in the following sequence:

1. Use an SSID that matches the AP.
2. Authenticate with the AP.
3. Use a packet encryption method (data privacy) *(optional)*.
4. Use a packet authentication method (data integrity) *(optional)*.
5. Build an association with the AP.

The following sections outline wireless communication, followed by an overview of wireless security. Chapter 4 is dedicated to a more robust explanation of wireless security and includes network security. As well, this chapter highlights other inter-related elements of security which may not be directly relevant to WLANs, however are integral to understanding and properly managing WLAN in K-12 school districts.

Wireless Signals

There are three wireless technologies and they are not interoperable. The three technologies are Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum and Infrared. Wireless technology standards are changing as testing verifies the capabilities and features of each product.

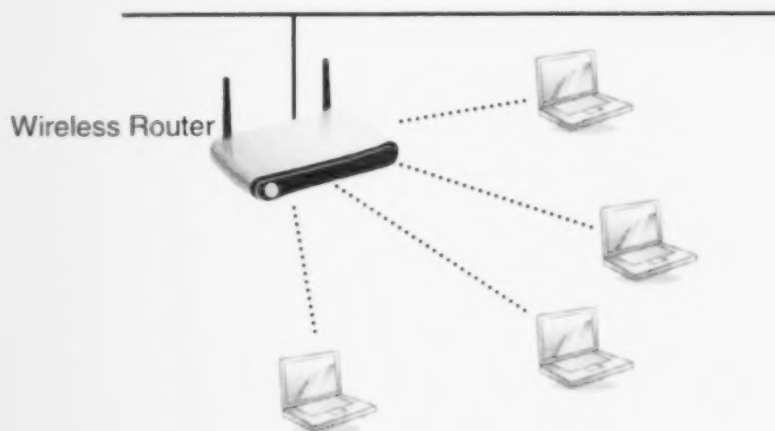
If two wireless signals are sent at the same time running on the same channel, they may collide and interfere with one another, requiring signals to be resent and ultimately slowing down the associated wireless process. Signals are literally floating through the air. These have the ability to bounce and redirect themselves, as well as to absorb themselves into their physical surroundings such as walls, floors, trees, people and the like.

SSIDs (Service Set Identifier)

In order to set up a wireless network for proper functionality, there are several required elements. These will vary depending on the level of security required for the network. There are two types of networks and they are referred to as a Basic Service Set (BSS) or an Independent Basic Service Set (IBSS). A BSS network consists of an Access Point or Wireless router as well as some client devices. An IBSS network consists of a group of clients connected to one another. All networks will have an SSID. This ensures that traffic between radios, whether an AP or client device, can be directed to the proper destination. On power-up, clients (such as a laptop) are typically looking for a network with a particular name. Some clients can be configured to look for a network with only one name; some clients like the Windows-XP client can be configured to connect to a variety of networks if the appropriate parameters have been configured in the utility. By default, the SSID is advertised by the AP in the beacon frame and is visible to most any client utility or network monitoring tool. Some network administrators restrict the advertising of the SSID or do not allow a client that does not know the name of the SSID to connect. When enabling this feature, care must be taken to ensure that the clients can tolerate this condition. Not all clients can connect to networks that do not advertise their SSID, even if it is known and programmed into the client.

The AP will also need a channel on which to operate. This channel will be dependent on whether you are operating in the 2.4 or 5.8 GHz band. Some APs have an option to look for the least congested channel, but in

most enterprise networks the administrator would plan out the channels for the network. The clients will scan all channels for the SSID and attempt to connect on the channel where the best signal is received. This scanning can be done in two ways. One is a passive scan where the client simply looks at the Beacon Frames on the channels and the second is by sending Probe Request frames to APs that it sees in the Beacon Frames and analyzing the information received in the Probe Response frame. The way in which a client accomplishes this is left to the vendor. Not all clients do this in the same way. Once the client has completed the scan if it has not yet sent the Probe Request, it will send a Probe Request Frame. upon receiving a Probe Response from the AP and processing what information it has gleaned from the Beacon Frame and the Probe Response frame, it then determines that nothing in these frames would prevent it from joining the network, it will send an Authentication Frame.



Basic Service Set - BSS

Basic Service Set, SAIT, Glen Kathler



Independent Basic Service Set - IBSS

Independent Basic Service Set, SAIT, Glen Kathler

Authentication and Association

This authentication process has nothing to do with the user of the device. The authentication just confirms that all layer 2 processes match between the client radio and the AP radio. The Authentication Response frame from the AP will indicate to the client whether it was successful in the authentication process.

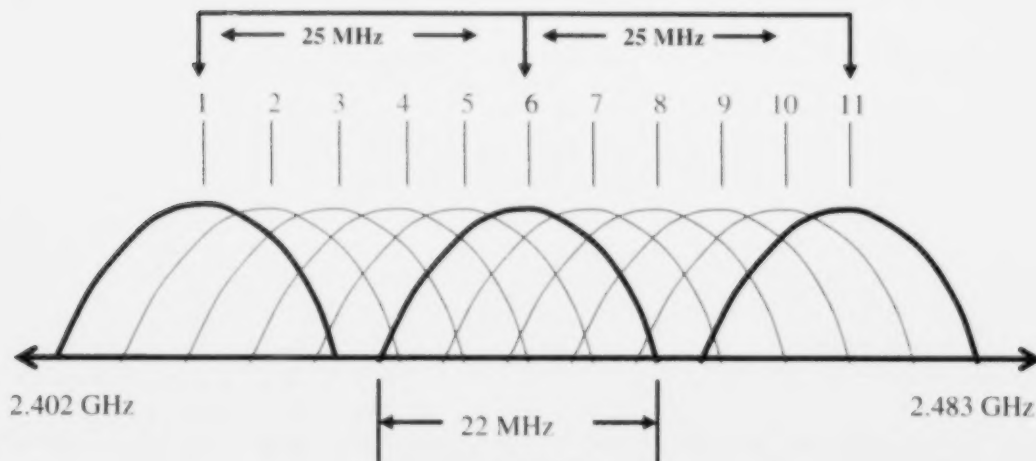
Once authentication is complete, the next step is Association, so the client sends an Association Frame and the Association Response Frame from the AP will indicate the success or failure of the process. Assuming a successful association to the AP if there was no 802.1X mechanism enabled, the client would be able to gain access to network resources including DHCP, Internet, and so on. If an 802.1X mechanism was enabled, the client would then need to complete the user authentication before network resources could be accessed.

Once a wireless client recognizes an Access Point or device transmitting beacon frames, it will attempt to authenticate with it. This authentication process is not to be confused with a user authentication that takes place prior to gaining access to the network's resources, but simply a layer 1 authentication. Do their layer settings match? These settings in their simplest form would be the Service Set ID (SSID), once these are confirmed in an exchange of frames consisting of beacon frames, probe request and probe response frames. Then an authentication frame exchange takes place. If this is successful, the client and Access Point proceed to the Association process.

At this stage the client typically scans all the channels to see if the SSID he has discovered is available on any other channels. If so, he will make some signal strength measurements and attempt to associate with the Access Point with the strongest signal. A client can theoretically be authenticated to multiple APs but associated to only one. The association frame exchange takes place with the AP of the client's choice. In the 802.11e or QoS versions, we will see the client make this decision on some additional information related to how busy the AP is how much traffic there is on a particular AP. The frame capture of a client attempting to associate to an AP is shown below. The first frame exchange is the probe request and probe response. This ensures that both devices are capable of the pending association. The client then proceeds with the authentication request, once the authentication response is received. The client will be reading the response for an accept indication, and it will then move on to the association request/response exchange. If this is successful then the client is allowed access to network resources or proceeds to some flavour of EAP authentication, if required.

Channels

The channels available for use in the various frequency bands and in conjunction with the different standards can be somewhat confusing. In the 2.4 GHz band there are 11 channels that can be used in North America. However they cannot all be used at the same time in the same location in an 802.11b or g network without interfering with one another. Channel 1 for example is 2.412 GHz and channel 2 is 2.417 GHz, a channel spacing of 5 MHz. However, an 802.11b or g system requires a minimum RF bandwidth of ≈ 22 MHz. The following figure shows the approximate RF bandwidth required for each channel.

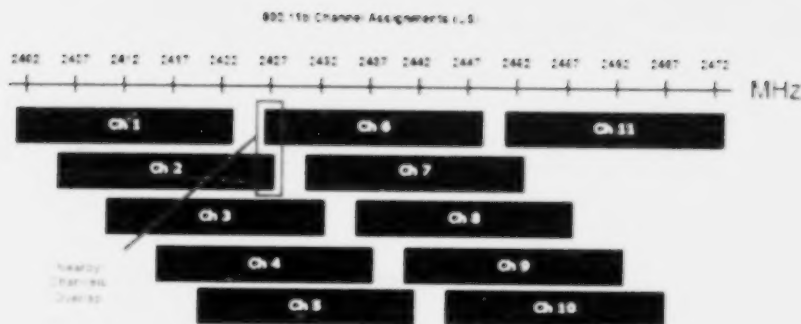


Channels, SAIT, Glen Kathler

The 5.8 GHz UNII band has been structured differently and the channel plan and bandwidth allocations have been designed with these applications in mind. For example, the UNII Low band between 5.15 GHz and 5.25 GHz has 4 non-interfering channels allocated. These are channels 36, 40, 44 and 48. With the UNII new band being added recently, there are 23 non-interfering channels available for 802.11a technology. The table below describes the UNII bands.

Table 3 - Channels and Bands, SAIT, Glen Kathler

Band (GHz)	Channels	Channel Numbers
UNII Low Band (5.15 - 5.25)	4	36,40,44,48
UNII Mid Band (5.25 - 5.35)	4	52,56,60,64
UNII New Band (5.470 - 5.725)	11	100,104,108,112,116,120,124,128, 132,136,140
UNII Upper Band (5.725 - 5.825)	4	149,153,157,161



Channel Assignment, SAIT, Glen Kathier

Collision Management

The radio channel is a shared medium. A collision occurs when two wireless waves of the same type (i.e. either IR, DSSS or FHSS) and frequency (i.e. on the same channel) intercept in mid-air. The colliding signals corrupt each other. Wireless networks must deal with the possibility of collisions just as wired networks do. However, the devices on the wireless network have no capability to determine if a collision has actually taken place. A carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) mechanism governs how the radio channel can be used. All 802.11 devices are half-duplex in nature and thus cannot listen and transmit at the same time. Due to these design criteria, the devices must attempt to avoid collisions altogether. Due to the mobile nature of a wireless network, there will be times when not all clients associated to a single AP can hear each other. This creates opportunities for collisions and the protocol behind CSMA/CA can help mitigate this. Some of the main differences between an 802.11 network and that of a typical wired 802.3 Ethernet network are:

- All frames carrying data on the 802.11 network must be acknowledged;
- Without the positive acknowledgement of a data frame the sender of the frame assumes a collision and resends the frame;
- The mechanism also provides a variety of mandatory wait times that all radio devices must use between the delivery of frames as well as when a device is waiting for the network to become available; and
- The mechanism also invokes a *random back-off timer* when the network is in use to ensure that all stations waiting for network access do so in an as orderly fashion as possible.

This process is what adds the majority of the reduction in throughput to the network. The balance of the reduction in throughput comes from the control and management frames required on the wireless network.

Several extensions of this mechanism exist, which are RTS/CTS as well as fragmentation. These are primarily used as optimization techniques for a Network Administrator in a network where more collisions and interference are present than normal.

There are two carrier sense mechanisms. One is a *physical carrier sense* which checks the Received Signal Strength Indication (RSSI). This determines if there are stations currently transmitting on the network as well as the ratio of the signal to the background noise on the channel. The other is a *virtual carrier sense* which uses a process called the Network Allocation Vector (NAV). This field is derived from the frames traversing the network which contain a duration field. This is data filled by the transmitting station to alert stations listening to the network as to how much time the network will be reserved for the current frame transaction. Once the NAV has been filled with a time value from the received duration field, the device immediately begins counting down until the NAV reaches zero. Only when the NAV is zero and the RSSI indicates the channel is clear can a wireless devices gain access to the channel.

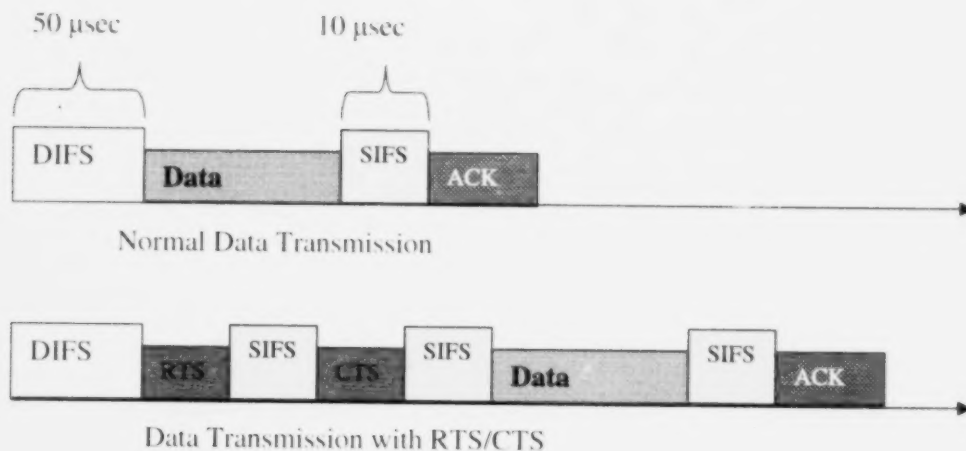
Inter-frame Spacing

These spaces are integral to the operation of a wireless network. There are primarily three of these spaces that affect the use of the wireless network.

The Short Inter-frame Space (SIFS) lasts 10 μ seconds. This space is mandatory between data frames and the required acknowledgement (ACK) frame. It is used following a Request-to-Send (RTS) frame that is used to reserve the network for a specific frame transaction. It is also used in a Clear-to-Send (CTS) frame which is the response to a RTS frame and allows this RTS/CTS transaction to occur without other stations gaining access to the network. This space is the shortest of all the inter-frame spaces.

The second of the inter-frame spaces in use is the Distributed Coordination Function Inter-frame Space (DIFS). Thank goodness for an acronym here! The DIFS lasts 50 μ seconds and is the time that must expire before any device can even begin to contend for the network.

The third space of concern is referred to as the slot time and is 20 μ seconds in duration. This is used during the random back-off timer when the network is in use. The station selects a random number and multiplies this against the slot time to determine how long the network must be idle before it can contend for the network. This is also the section of the standard that has been modified by 802.11e QoS functionality. By altering these values, various types of media frames such as voice and video can achieve a higher priority than that for best-effort data, management and control frames.



Interframe Spacing, SAIT, Glen Kathler



The radio channel is a shared medium. A collision occurs when two different waves of the same type (i.e., either IR, DSSS or FHSS) and frequency rise on the same channel at the same time. The colliding signals corrupt each other. Wireless networks must deal with the possibility of collisions and as wired networks do. However, the devices on the wireless network have no capability to determine if a collision has actually taken place. A carrier-sense Multiple Access/Carrier Avoidance (CSMA/CA) mechanism governs how the radio channel can be used. As 802.11 protocol was first designed to support infrastructure-based and later extended to support ad hoc networks, these two devices must attempt to avoid collisions altogether. In any of the radio types, if a network network, there are stations present or users connected to a single AP can hear each other. This makes it difficult for collisions and the protocol before CSMA/CA can help mitigate this. Some of the major differences between 802.11 networks and that of a typical wired 802.3 Ethernet network are:

- Frames carrying data on the 802.11 radio have to be acknowledged.
- Without the positive acknowledgment of a data frame, the sender of the frame generates a "retry" or resends the frame.
- The mechanism also provides a variety of regulatory restrictions that governs how the radio must use because the diversity of those as well as when a device is working in the network to be used available. (1)
- The mechanism also includes a random back-off time. After the network is in use to determine if stations capable for network access are in an appropriate channel as possible.

One process is deal with the property of the radio that it is subject to the network. The process of the channel is a traditional method from the control and management frame depend on the previous example.

Several extensions of this mechanism exist, which are IEEE 802.11 as well as 802.11p. These are primarily used as optimization techniques for a Network Admission Control (NAC) network where more collisions and other factors are present than normal.

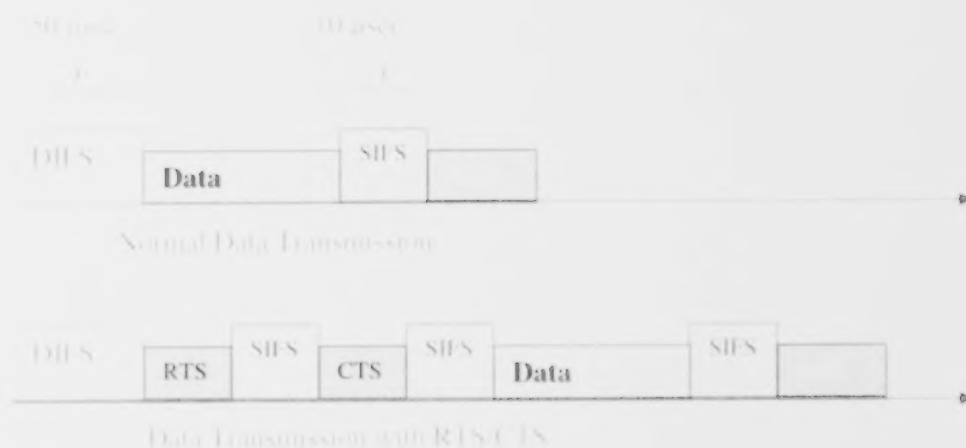
There are two carrier sense mechanisms. One is a physical carrier sense which is called the Received Signal Strength Indication (RSSI). This determines if there are stations currently transmitting on the network as well as the ratio of the signal to the background noise on the channel. The other is a virtual carrier sense which uses a process called the Network Allocation Vector (NAV). This field is derived from the frames traversing the network which contain a duration field. This is data field by the transmitting station to set stations entering to the network as to how much time the network will be reserved for the current frame transmission. Once the NAV has been filled with a time value from the received duration field, the device immediately begins counting from when the NAV reaches zero. Only when the NAV is zero and the RSSI indicates the channel is clear can a wireless device gain access to the channel.

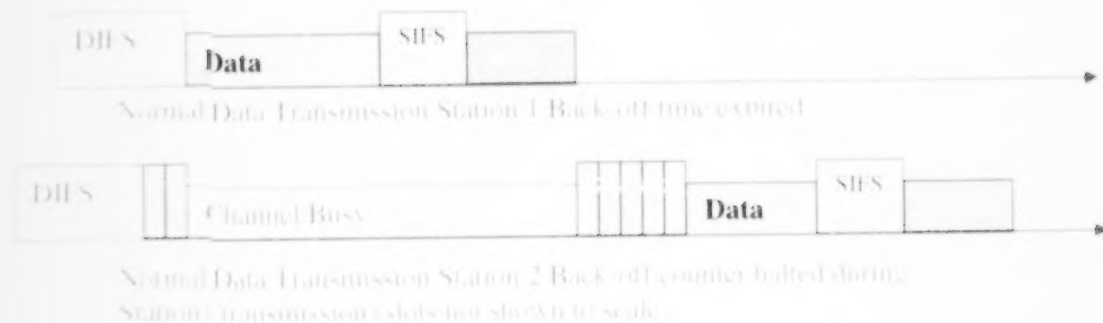
These spaces are integral to the operation of a wireless network. There are primarily three of these spaces that affect the use of the wireless network:

The Short Inter-frame Space (SIFS) lasts 10 microseconds. This space is mandatory between data frames and the required acknowledgement (ACK) frame. It is used following a Request-to-Send (RTS) frame that is used to reserve the network for a specific frame transaction. It is also used in a Clear-to-Send (CTS) frame which is the response to a RTS frame and allows this RTS/CTS transaction to occur without other stations gaining access to the network. This space is the shortest of all the inter-frame spaces.

The second of the inter-frame spaces in use is the Distributed Coordination Function Inter-frame Space (DIFS). Thank goodness for an acronym here! The DIFS lasts 50 microseconds and is the time that must expire before any device can even begin to contend for the network.

The third space of concern is referred to as the slot time and is 20 microseconds in duration. This is used during the random back-off time when the network is in use. The station selects a random number and multiplies this against the slot time to determine how long the network must be idle before it can contend for the network. This is also the section of the standard that has been modified by 802.11e QoS functionality. By altering these values, various types of traffic frames such as voice and video can achieve a higher priority than that for best-effort data management and control frames.



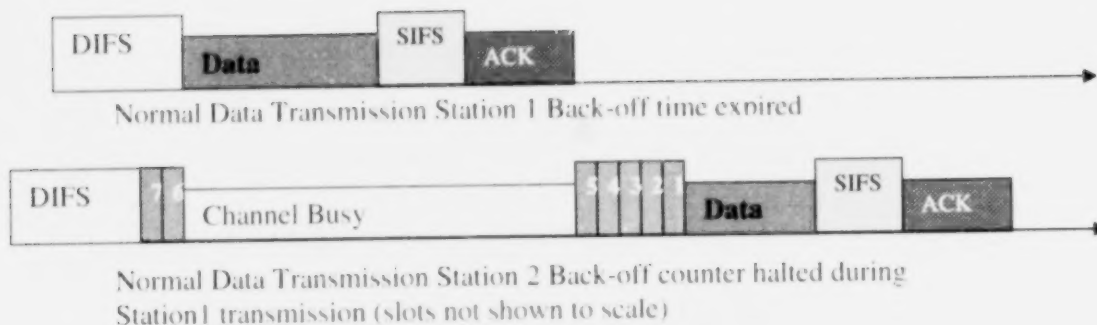


The operation of a wireless network needs to ensure that any network responds rapidly when the Industry Canada regulations for Effective Isotropic Radiated Power (EIRP). This is how much power the respective device and its antenna system are radiating into free space. Industry Canada governs the use of all radio spectrum. Even though the 800 MHz bands are unlicensed, they are subject to the specific rules set out by Industry Canada. The other item that is regulated is the Intermodulation Interference (IMI) the amount of RF energy that is being fed into the antenna. The IMI power limit is set at 1 Watt or 30 dBm.

Wireless networks are typically categorized into two families: point-to-point configuration and the other is point-to-multipoint configuration. The point-to-point configuration is typically used in the example of a wireless bridge link. This is where two sections of network need to connect and the solution chosen is a wireless bridge. Here the two wireless devices use a very directional, narrow beam width antenna and are equipped a higher EIRP than the point-to-multipoint system. If the antennas chosen are of an omnidirectional type (these will have a radiation pattern of 360°) the system is automatically governed by the point-to-multipoint rules. The maximum allowed EIRP for a point-to-multipoint system is 36 dBm or 4 Watts.

Using the maximum RF power of 30 dBm and the maximum allowed EIRP of 36 dBm, the system using a maximum antenna gain of 36 dBm $\div$ 30 dBm = 6 dB. The gain of an antenna which is measured with respect to a theoretical antenna (the isotropic radiator, therefore the term dBi). For every additional 3dB of additional antenna gain added to this system, the RF power must be reduced by 3dB below the initial +30 dBm. Antenna manufacturers typically build their antennas in multiples of 3 dB of gain. So these are the rules for point-to-multipoint systems.

If a system is determined to be a point-to-point system with very directional, narrow beam width antennas, then the rules are slightly different. In this case for every additional 3dB of antenna gain above the initial 6 dB the power of the RF must be reduced by 1dB from the initial +30 dBm. This allows point-to-point to be regulated that can cover distances in the 30 to 50 km range depending on the antenna and RF power density. There is some additional relaxation of these rules in the UNII-3 band 5.725 $\div$ 5.825 GHz. This band, which is primarily for point-to-point links allows antennas with a directional gain up to 23 dBi before any reduction in RF power is required. This allows point-to-point links an EIRP of 200 Watts.



Interframe Spacing 2, SAIT, Glen Kathler

Power

The operator of a wireless network needs to ensure that all network devices operate within the Industry Canada regulations for Effective Isotropic Radiated Power (EIRP). This is how much power the respective device and its antenna system are radiating into free space. Industry Canada governs the use of all radio spectrum. Even though the 802.11 bands are license-free, they still fall under the specifications set out by Industry Canada. The other item that is regulated is the Intentional Radiator (IR), this is the amount of RF energy that is being fed into the antenna. The IR power limit is set at 1 Watt or 30 dBm.

Wireless networks are typically categorized into two families - one is a point-to-point configuration and the other a point-to-multipoint configuration. The point-to-point configuration is typically used in the example of a wireless bridge link. This is where two sections of network need connectivity and the solution chosen is a wireless bridge. Here the two wireless devices use a very directional, narrow beam width antennae and are allowed a higher EIRP than the point-to-multipoint system. If the antennae chosen are of an omni-directional type (those with a radiation pattern of 360°) the system is automatically governed by the point-to-multipoint rules. The maximum allowed EIRP for a point-to-multipoint system is 36 dBm or 4 watts.

Using the maximum IR power of 30 dBm and the maximum allowed EIRP of 36 dBm, this would allow a maximum antenna gain of $36 \text{ dBm} - 30 \text{ dBm} = 6 \text{ dBi}$. The gain of an antenna which is passive is measured with respect to a theoretical antenna (the isotropic radiator) therefore the term dBi. For every additional 3dBi of additional antenna gain added to this system, the IR power must be reduced by 3dB below the initial +30 dBm. Antenna manufacturers typically build their antennae in multiples of 3 dBi of gain. So these are the rules for point-to-multipoint systems.

If a system is determined to be a point-to-point system with very directional, narrow beam width antennae, then the rules are slightly different. In this case for every additional 3Bi of antenna gain above the initial 6 dBi the power of the IR must be reduced by 1dB from the initial +30 dBm. This allows point-to-point to be installed that can cover distances in the 30 to 50 km range depending on the antennae and IR power chosen. There is some additional relaxation of these rules in the UNII-3 band 5.725 – 5.825 GHz. This band, which is primarily for point-to-point links allows antennae with a directional gain up to 23 dBi before any reduction in IR power is required. This allows point-to-point links an EIRP of 200 Watts.

2.2 Wireless Security Standards

Wireless network traffic flows in an open medium, the air interface, and must be considered insecure. A network administrator must be aware of the types of security risks there are, as well as some of the solutions available to mitigate those risks. Some of the attacks against a wireless network cannot be prevented and only effective monitoring of the network and proper responses will reduce the risk associated with the wireless portion of a network. In most cases, the role of wireless in the network is to create access to a network already in place or the Internet. So some form of authentication and segmentation is required to manage who gets access to specific network resources. As wireless technology is introduced into enterprises where security is mandatory, wireless traffic needs to be secure.

CIA is an often used acronym to describe the requirements of a wireless security solution.

C – Is the data on the network being kept as **Confidential** as it needs to be?

I – Is the network maintaining its **Integrity**?

A – Are the users on the network who they are supposed to be? Have they been **Authenticated**?

First generation 802.11 wireless devices were expensive, scarce and users were not particularly concerned with security. Wired Equivalent Privacy (WEP) was incorporated into the original standard as it was thought to provide just that.

Security in all networks is woven into the security policy of the enterprise. How sensitive is the data on the network? What are the risks if data is compromised? What defines acceptable use? As well, it is usually combined with an authentication scheme to provide not only authorized use but effective encryption. Most of the existing wired network user authentication methods can be leveraged over a wireless network.

As a client brings up its wireless connection, it must find an AP that is reachable and that will approve its membership. The client must negotiate its membership and security measures in the following sequence:

1. Use an SSID that matches the AP.
2. Authenticate with the AP.
3. Use a packet encryption method (data privacy) (*optional*).
4. Use a packet authentication method (data integrity) (*optional*).
5. Build an association with the AP.

Packet Encryption and Authentication

Two basic concerns that 802.11 clients and APs must work out are authentication and encryption. These are the basic two elements of wireless security. Authentication verifies the content of the packets of information travelling between two trusted wireless devices, such as a laptop and an AP. Next, encryption ensures that only the two trusted, wireless devices can read the information.

Many different methods are available for authentication, encryption and a combination of the two. The sections that follow briefly describe these methods.

EAP and 802.1X Authentication Protocols

Wireless security has evolved to use additional, more robust methods. APs can use a variety of authentication methods that leverage external authentication and authorization servers and their user databases. The Extensible Authentication Protocol (EAP) forms the basis for many wireless security methods, most of which have similar acronyms, such as EAP, PEAP, and LEAP.

Because EAP is extensible, it is well suited for a variety of secure environments. EAP has its history in Point-to-Point-Protocol (PPP, also known as *dial up*) communication, not in wireless authentication.

Described above is the IEEE 802.1X protocol as port-based authentication, or the means to authenticate users to use switch ports. Through 802.1X, users can authenticate even at Layer 2, before gaining further network connectivity. WLANs can leverage 802.1X as the means to implement EAP at Layer 2 for wireless clients. In a wireless LAN, you can find some of the following security method names: LEAP, PEAP, EAP-TLS, and EAP-FAST. So many different methods exist that it is becoming confusing about what they are and what they do.

Just remember that each one is based on EAP and uses a different type of credentials to authenticate wireless users. Some of the EAP-based methods go beyond authentication by adding extra security features and is outlined below.

EAP-TLS

The EAP-TLS method uses the Transport Layer Security (TLS) protocol to secure client authentication. TLS is based on Secure Socket Layer (SSL), which is commonly used in secure web browser sessions. EAP-TLS uses digital certificates as authentication credentials, which means that every AP and wireless client must have a certificate generated and signed by a common certificate authority (CA). EAP-TLS also addresses wireless data privacy by generating WEP keys automatically, each time the authentication server forces the client to re-authenticate. The TLS session key, unique to each wireless client that is authenticating, is used to derive a unique WEP key. The WEP key is then used to encrypt the wireless data.

PEAP

Protected EAP (PEAP or EAP-PEAP) is similar to EAP-TLS in that a TLS session is used to secure the authentication. PEAP requires a digital certificate only on the authentication server so that the server itself can be authenticated to the client. The wireless clients are authenticated using Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2). As with EAP-TLS, the TLS session key is used to derive a WEP key for encrypting the wireless data stream. The keys change periodically as the authentication server forces the client to re-authenticate.

EAP-FAST

EAP Flexible Authentication via Secure Tunneling (EAP-FAST) is a wireless security method developed by Cisco. EAP-FAST is not named for its speed; rather, it is named for its flexibility to reduce the administrative complexity. Clients are not required to use digital certificates, and they are not required to follow strict or strong password policies. EAP-FAST works by building a secure tunnel between the client and the authentication server. A Protected Access Credential (PAC) is used as the only client credential to build the tunnel. The PAC can be assigned from a PAC server or it can be created dynamically during a phase of EAP-FAST negotiations. Once the tunnel is built, the client is authenticated using familiar username and password credentials. EAP-FAST can derive a WEP key dynamically so that the wireless data stream can be encrypted.

Comparison of EAP Methods

Table 4 - Comparison of EAP Methods, SAIT, Glen Kathler

Authentication Protocol -->	EAP-MD5	EAP - LEAP	EAP- TLS	TTLS (EAP-MSCHAPv 2)	PEAP (EAP-MSCHAPv 2)	PEAP (EAP-TLS)	PEAP (EAP-GTC)	EAP-FAST
802.1X Authentication Characteristics								
Port-based	No	No	Yes	No	No	Yes	No	No
Server authentication	No	No	Yes	Yes	Yes	Yes	Yes	No
Client authentication	No	Yes	N/A	Yes	Yes	No	Yes	Yes
Security	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Encryption	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authentication	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authorization	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Accounting	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

802.1X

Upon detection of the new wireless client, the "supplicant", the port on the switch, the "authenticator", is enabled and set to the "unauthorized" state. In this state, only 802.1X authentication traffic will be allowed. Other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The authenticator will send out the EAP-Request identity to the supplicant, the supplicant will then send out the EAP-response packet that the authenticator will forward to the authenticating server, usually a RADIUS server (Remote Authentication Dial In User Service). The authenticating server can accept or reject the EAP-Request. If it accepts the request, the authenticator will set the port to the "authorized" mode and normal traffic such as HTTP will be allowed. When the supplicant logs off, an EAP-logoff message is sent to the authenticator. The authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

In the WLAN world, 802.1X by itself is a Port-based Access Control, a flexible authorization scheme that can work with WPA, WPA2 or 802.11i technologies. It is typically combined with an authentication protocol, and as a pair they provide a secure authentication and encryption key rotation mechanism.

Not all hardware supports 802.1X. You may be required to upgrade Network Interface Cards (NICs), APs, Switches or other hardware to implement 802.1X.

WLAN Authentication and Encryption

In 802.11 networks, clients can authenticate with an AP using many methods. The following are some of the most common means of connecting to a WLAN. It is worth noting that the level of security provided varies under the different methods. These methods are listed in order of the level of security which they provide, starting with the oldest and generally accepted as least secure.

Open authentication

No authentication method is used. Any client is offered open access to the AP.

Status: This is insecure and not suitable for K-12 school environments.

Pre-shared key (PSK)

The same secret key is statically defined on the client and the AP. If the keys match, the client is permitted to have access. Notice that the authentication process in these two methods stops at the AP. In other words, the AP has enough information on its own to independently determine which clients can or cannot have access. Open authentication and PSK are considered to be legacy methods because they are not scalable and are not necessarily secure. Open authentication is usually the default, and offers no client screening whatsoever. Any client is permitted to join the network without presenting any credentials. In effect, the SSID is the only credential that is required. Although this makes life easier, it does not do much to control access to the WLAN. In addition, open authentication does not provide a means to encrypt data sent over the WLAN.

Pre-shared key authentication uses a long Wireless Equivalence Protocol (WEP) key that is stored on the client and the AP. When a client wants to join the WLAN, the AP presents it with a challenge phrase. The client must use the challenge phrase and the WEP key to compute a value that can be shared publicly. That value is sent back to the AP. The AP uses its own WEP key to compute a similar value. If the two values are identical, the client is authenticated.

When pre-shared key authentication (commonly called *static WEP keys*) is used, the WEP key also serves as an encryption key. As each packet is sent over the WLAN, its contents and the WEP key are fed into a cryptographic process. When the packet is received at the far end, the contents are unencrypted using the same WEP key.

Pre-shared key authentication is more secure than open authentication, but it has two shortcomings:

- It does not scale well because a long key string must be configured into every device; and
- It is not very secure.

As you might expect, a static key persists for a very long time, until someone manually reconfigures a new key. The longer a key remains in use, the longer malicious users can gather data derived from it and eventually reverse-engineer the key. It is commonly known that static WEP keys can be broken.

Status: This is insecure and not suitable for K-12 school environments.

WEP

Wired Equivalent Privacy was incorporated into the original standard as a means to encrypt the traffic on the network. From the wireless vendors perspective, it was easy to implement, did not require much CPU power to encrypt and decrypt traffic, exportable, self-synchronizing and used a relatively strong cipher. The weakness that has been exploited is related to the fact that a static key entered in both the Access Point and the client is required. This key is only changed manually, typically by an administrator of the devices, and must match on both devices. With these static keys being used to encrypt traffic on the network, an intruder can capture encrypted traffic and then run the traffic against an encryption cracking software or now even orchestrate a live encryption key cracking event on a network that employs this security mechanism.

Status: This choice is vulnerable. Avoid use as the only means of WLAN security for school networks, because vulnerabilities and cracking tools have been published. If WEP must be used, it should be configured for 128-bit encryption, and passwords must have a high degree of entropy.

Status: Overall, this is insecure and not suitable for K-12 school environments.

WPA

Wi-Fi Protected Access was initially a stop-gap measure implemented by the Wi-Fi Alliance to provide an interim security option during the time that 802.11i was under development. It actually repairs the primary weakness in WEP with a mechanism to rotate the encryption keys periodically and removes any requirements from the Administrator or user to manually enter an encryption key. It also allows for each device to use a unique encryption key rather than sharing the same key with all the other users on this Access Point. The two methods of creating the key to be used for encryption are first of all a Passphrase method. This method once again requires a manual entering of an 8 to 63 character passphrase in both the Access Point and the client. The passphrase must match in all devices using this Access Point. As a client connects to the Access Point, the client and AP go through a process called a four-way handshake to derive the encryption key for that client. The passphrase then is the weak link in this method and there are already software tools that can be used to derive the passphrase from a captured four-way handshake. This can be mitigated to some degree by a strong passphrase. WPA offers the following wireless LAN security measures:

- Client authentication using 802.1X or a pre-shared key;
- Mutual client-server authentication;
- Data privacy using Temporal Key Integrity Protocol (TKIP); and
- Data integrity using Message Integrity Check (MIC).

TKIP leverages existing WEP encryption hardware that is embedded in wireless clients and APs. The WEP encryption process remains the same, but the WEP keys are generated much more frequently than the periodic re-authentications that occur with EAP (Extensible Authentication Protocol, defined further in following pages) based authentication methods. In fact, TKIP generates new WEP keys on a per-packet basis. An initial key is built as a client authenticates (or re-authenticates) with the EAP-based method. That key is formed by mixing the MAC address of the transmitter (the client or the AP) with a sequence number. Each time a packet is sent, the WEP key is incrementally updated. Once the client is forced to re-authenticate, an entirely new WEP key is built and the per-packet process repeats. WPA can use a pre-shared key for authentication if external authentication servers are not used or required. In that case, the pre-shared key is used only during the mutual authentication between the client and the AP. Data privacy or encryption does not use that pre-shared key at all. Instead, TKIP takes care of the rapid encryption key rotation for WEP encryption. The MIC process is used to generate a "fingerprint" for each packet sent over the wireless network. If the fingerprint is made just before the packet is sent, the same fingerprint should match the packet contents once the packet is received. Why bother fingerprinting packets in the first place? When packets are sent over the air, they can be intercepted, modified, and re-sent—something that should never be allowed to happen. Fingerprinting is a way to protect the integrity of the data as it travels across a network. For each packet, MIC generates a hash code (key), or a complex calculation that can only be generated in one direction. The MIC key uses the original unencrypted packet contents and the source and destination MAC addresses in its calculation, so that these values cannot be tampered with along the way.

Status: The recommended usage for this type of encryption is in the small office/home office (SOHO) and consumer use environment.

Not all hardware supports WPA. You may be required to upgrade Network Interface Cards (NICs), APs or other hardware to migrate from WEP, PSK or open authentication to WPA.

WPA2

Wi-Fi Protected Access version 2 (WPA2) is based on the final 802.11i standard. WPA2 goes several steps beyond WPA with its security measures. For data encryption, the Advanced Encryption Standard (AES) is used.

AES is a robust and scalable method that has been adopted by the National Institute of Standards and Technology (NIST, www.nist.gov) for use in the U.S. government organizations. TKIP is still supported for data encryption, for backward compatibility with WPA. With WPA and other EAP-based authentication methods, a wireless client has to authenticate at each AP it visits. If a client is mobile, moving from AP to AP, such as a student with a tablet PC walking throughout the school requiring constant connectivity to the WLAN, the

continuing authentication process can become cumbersome. WPA2 solves this problem by using Proactive Key Caching (PKC). A client authenticates just once, at the first AP it encounters. As long as other APs visited support WPA2 and are configured as one logical group, the cached authentication and keys are passed automatically.

Status: Superior security over WPA and the minimum recommended level of WLAN security for a K-12 school environment.

Not all hardware supports WPA2. You may be required to upgrade Network Interface Cards (NICs), APs and/or other hardware to migrate from WPA to WPA2.

WPA/WPA2 Personal vs. Enterprise

Within the above described WPA and WPA2 authentication/encryption methods, there are two further types. The first type is known as personal and the other is referred to as enterprise. The primary difference between these two types is that Personal does not use EAP or a server such as RADIUS to authenticate users. Personal stores all security settings within the APs themselves. Enterprise uses EAP to facilitate authentication with an authentication server such as RADIUS. Variations of these methods are described next.

WPA Personal mode and WPA2 Personal mode do not use an EAP type and a managed authentication server such as RADIUS. Instead, they work from a static list of keys stored in the access point. Avoid use on company networks because vulnerabilities and cracking tools have been published. If PSK must be used, passwords must have a high degree of entropy.

In an enterprise environment, some flavour of authentication is needed whereby users are required to authenticate to a Server, an Active directory, RADIUS, LDAP data base or some other type of resource that maintains the users and their credentials. This eliminates the weakness of the passphrase in WPA-PSK. There are three elements of this process - Supplicant (Client), Authenticator (AP) and the Authentication Server (AS). In some enterprise APs, the Authentication Server may reside in the AP. Typically, once that process is complete the server and the client determine the encryption key for that user and that specific session. The AS then sends the encryption key to the Authenticator for use in that specific session. WPA still uses a WEP key, but each client has their own encryption key. WPA2 assigns a unique key for each client, however, it uses the AES encryption mechanism.

Both WPA/WPA2 Personal and Enterprise are among the strongest level of security available today.

Use Enterprise over Personal for its superior centralized control and management of user authentication credentials.

WPA Enterprise Mode with EAP-TLS or PEAP for Authentication and TKIP for Encryption

Status: If using WPA, this is amongst the strongest level of protection currently available. WPA with TKIP is a suitable alternative to WPA2 while waiting to migrate to new equipment. EAP-TLS is the most thoroughly tested authentication protocol for interoperable security. Some forms of PEAP may be easier to implement because client-side certificates are optional. However, variations exist between implementations by Cisco, Microsoft and other vendors. TKIP resolves the encryption vulnerability found in WEP.

WPA2 Enterprise Mode with EAP-TLS or PEAP for Authentication and TKIP for Encryption

Status: Amongst the strongest level of protection currently available. Alternative to WPA2, with TKIP for encryption to accommodate small devices. TKIP resolves the encryption vulnerability found in Wired Equivalent Privacy (WEP). This option must be considered for smaller devices that can support WPA2 authentication, but lack the processing power for AES.

WPA2 Enterprise Mode with EAP-TLS or PEAP for Authentication and AES for Encryption

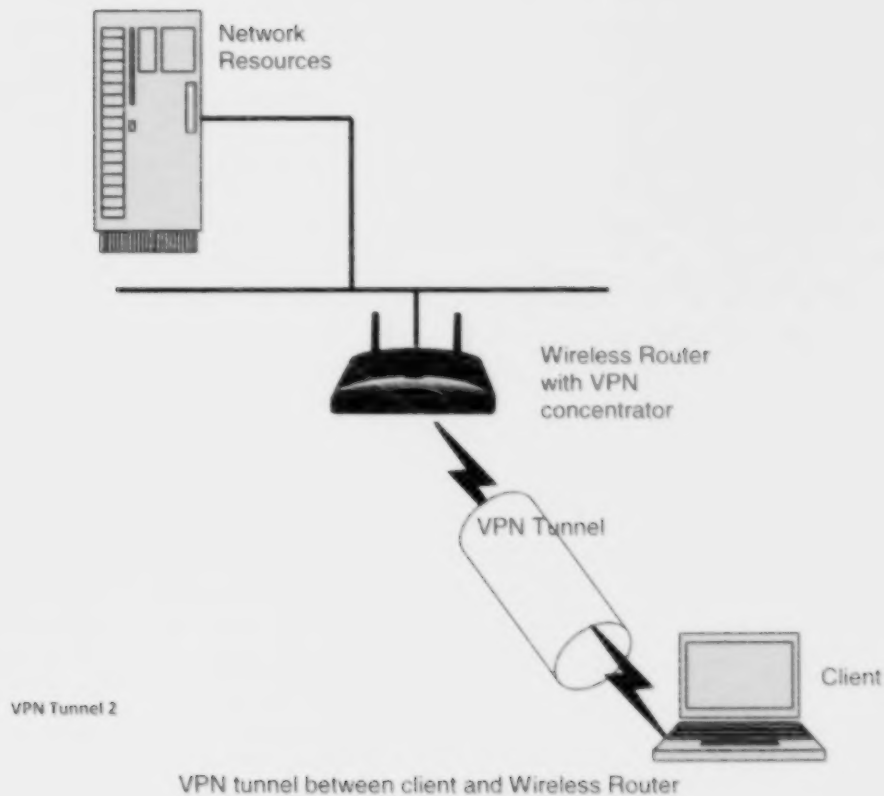
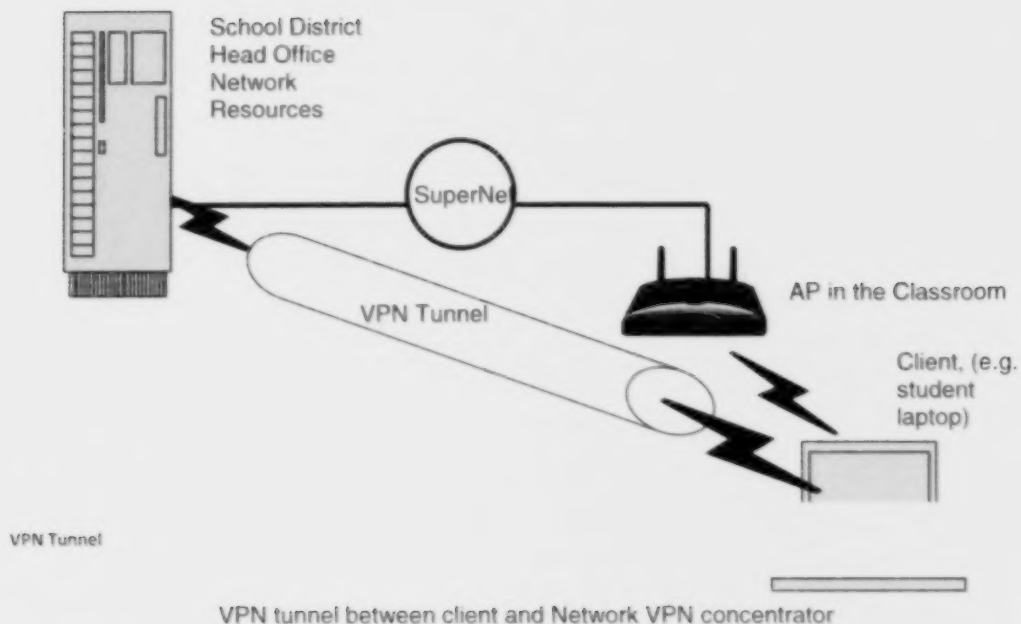
Status: The strongest level of protection currently available. WPA Enterprise mode uses an EAP type in conjunction with an authentication server. EAP-TLS, one of several EAP types, is the most thoroughly tested authentication protocol for interoperable security. Some forms of PEAP, a newer EAP type, may be easier to implement because client-side certificates are optional. However, variations exist between implementations by Cisco, Microsoft and other vendors.

Virtual Private Network (VPN)

In addition to the previously described authentication and encryption methods, it has become commonplace to add VPN technology as an additional layer of security for mobile devices.

If students are taking laptops off school grounds and require access to the Internet or other one-to-one school resources, VPN technology is highly recommended. It will allow you to control and monitor content while protecting students. See Chapter 4 for more details.

Virtual Private Network (VPN) technology has existed since the days of Remote Access for dial-in modem connections to the corporate network. This technology can be implemented in Wireless Networks as well. It can provide encryption, tunnelling and security when a wireless client gains access to an unsecured network such as a local hotspot. Prior to the client gaining access back to his corporate network, he is required to authenticate in some manner against a VPN concentrator at the corporate headquarters. A tunnel and encryption can then be setup between the concentrator and the client to secure the transport of packets between them over an un-secure network such as a wireless connection. Some wireless routers are also capable of acting as the VPN concentrator or endpoint. This allows clients to establish a secure tunnel between itself and the wireless router.

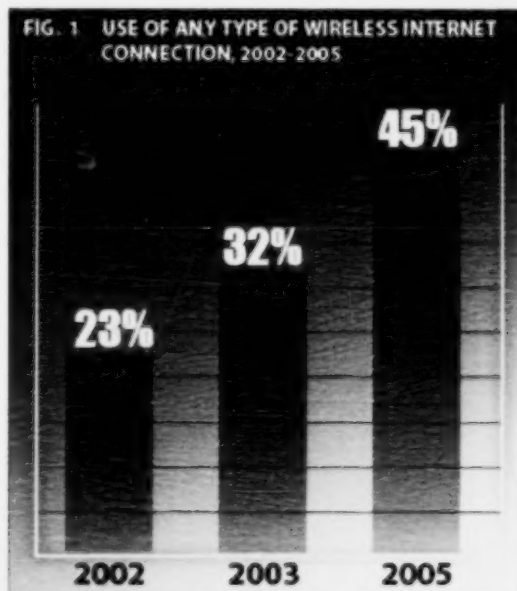


2.3 Overview of Wireless Market and Vendors

This section provides you a snapshot of the wireless market today, including insight into the adoption of WLANs into K-12 schools. Information from several vendors is included, although this is not an endorsement of any particular vendor, whether they are listed or not.

Market Overview

A recently released American study on Internet access showed dramatic growth in wireless Internet access in public schools in 2005. All told, 45% of public schools in 2005 used some form of wireless Internet access, a growth of more than 40% over 2003, in which only 32% of public schools had wireless access.



Source: NCES survey: Internet Access in U.S. Public Schools and Classrooms: 1994–2005, published November 2006.

WLANs in US Schools, NCES survey, 2006

In 2005, 45% of elementary schools had some sort of wireless Internet access, up from 29% in 2003. Secondary schools came in ahead of elementary schools at 48% in 2005, but the increase from 2003 was slighter, up just six points from 42%.

Alberta's Education System and Adoption of WLANs

Although concise data has not been gathered for this guide, a reasonable estimate can be made from discussions with a sample of districts. The consensus is that the majority of Alberta school jurisdictions have at least dipped their toe into the water of WLAN procurement, implementation and management. However, there are still many districts without any wireless experience to date.

The case studies at the end of this guide provide for a summary of three districts' experiences with WLANs.

Market Description

WLANs are becoming a standard part of school networks. One of the biggest driving factors is one-to-one wireless learning initiatives delivering education to students with laptops, PDAs (Personal Digital Assistants), tablets, iPads and other devices. There are a vast number of manufacturers, OEM partners and resellers providing solutions in Canada today. The overwhelming trend for business customers, as well as K-12 schools, is moving toward APs with wireless controllers for their WLAN architecture, also referred to as *thin* APs. However, small offices and schools continue to deploy fully functional stand-alone access points, also referred to as *thick* APs.

If only deploying, and planning on scaling to a small number of APs at any given school, then thick APs can be a suitable solution. However, for larger deployments and scalable solutions with the most efficient *remote, centralized* management capabilities, *thin* AP solutions are becoming the standard.

Three key reasons for deploying wireless LANs are:

1. Increased productivity;
2. Broadening access areas where cost or physical barriers have limited traditional wired networks; and
3. Improved efficiency in specific processes.

Technically, WLANs are considered quite secure today, so long as they are correctly specified (i.e. optimal hardware and software for the specific application), configured and managed. Due to the adoption of IEEE standards and overall improvements to wireless technology, wireless is now being deployed behind the firewall opposed to being an off shoot of the infrastructure, as it was in its infancy.

The manufacturer-specific security solutions offered have started to raise the wireless authentication framework as an issue that must be considered. However, lack of total interoperability is still a barrier to simple deployment. One of the biggest concerns is with the increased scope of network management. This support often requires additional skills training for existing staff.

Previously, locations (such as a branch office or individual school site) were identified as a network node. Now it is demanded that each and every device (used by employees, teachers or students) is identified as a node on a wired or wireless network. Now every major physical item owned is becoming a node on a network empowering IT departments to increase control and management right down to the desktop and application layer.

The enterprise WLAN infrastructure market is comprised of a vast number of high and low-risk vendors with varied capabilities and company sizes. The best vendors will provide the widest array of options to tailor to a district's needs at the optimum price points. They will also offer flexible security and strong management tools. The good news is that the functions offered by the various vendors are narrowing to the core set described in this guide.

Some vendors are stand-alone WLAN vendors that provide their technology as a non-invasive overlay to an existing wired network. Others possess a family of wired products that are highly integrated with the WLAN products. Where the latter exists, the best vendors have provided a single management console to control both network types.

Market Definition/Description

The WLAN infrastructure market consists of vendors that provide wireless IP networking solutions that conform to IEEE 802.11 standards through the Wi-Fi Alliance certification process. The core components of any WLAN vendor are:

1. Access Points (APs) – each including radio(s) and antenna(e)
2. Controllers
3. Centralized Management Software

In very simple terms, APs are what the individual devices (wireless laptops, PDAs or “clients” connect to), and Controllers consolidate functions for Centralized Management Software to perform updates and configuration of APs (without the necessity of having to physically go to each and every AP).

All APs that contain a minimum of two radios that can act either as service link radios or as air sensors for security purposes. All radios are typically configurable across any of the bands in the aforementioned frequencies. Each radio supports multiple Basic Service Set Identifiers (BSSIDs). More advanced APs support the additional capability to use one of the radios for wireless backhaul and, in the more advanced systems, capability as a mesh networking vendor, however no “mesh-only” vendors are included in this section.

Vendors also provide a variety of antennae — from those that give simple diversity, to multiple input, multiple output (MIMO), to higher gain antennae that provide increased or focused coverage.

Virtually all incumbent wired LAN manufacturers have already launched WLAN products. Despite what the name says on the equipment itself, the actual solution is either their own or provided via an Original Equipment Manufacturer (OEM) partnership with another manufacturer. Vendors manufacturing and marketing their own solutions as well as those who have done so with an OEM Partner are listed in the following section.

Vendors

Based on disclosed information from vendors available in the marketplace, and general industry knowledge, the following OEM partner relationships are known. These relationships should be verified should they become material to any critical decision or product acquisition. Each vendor is shown, followed by its website for additional contact information, and its OEM partner (shown as not applicable [NA] where relevant).

Table 5 - Vendor Websites and OEM Relationships

Vendor	Website Address
3Com	www.3com.com
Alcatel-Lucent	www.alcatel-lucent.com
Aruba Networks	www.arubanetworks.com
Bluesocket	www.bluesocket.com
Cisco Systems	www.cisco.com
Colubris	www.colubris.com
Enterasys Networks	www.enterasys.com
Extricom	www.extricom.com
Extreme Networks	www.extremenetworks.com
Foundry Networks	www.foundrynet.com
Hewlett-Packard	www.hp.com
Meru Networks	www.merunetworks.com
Nortel Networks	www.nortel.com
Siemens	www.siemens.com
Symbol Technologies / Motorola	www.symbol.com
Trapeze Networks	www.trapezenetworks.com
Vernier	www.vernier.com
Xirrus	www.xirrus.com

The scope of this guide does not allow for a thorough review and inclusion of product information from all vendors. Please use the above website information to research additional vendor information.



© Guillaume Morel - Fotolia.com

- First Steps
 - Setting Realistic Goals and Expectations
 - Team, Roles and Responsibilities
 - Specific One-to-One Initiative Considerations
- Analysis
 - Immediate Scope and Future Scalability
 - Budget Requirements and Limitations
 - Technology Selection
- Project Plan
 - Timeframe
 - Scope
 - Labour
- Technical Deployment Considerations
 - Network
 - Internet Connectivity
 - Site Survey
 - Signal Strength
 - Impact of Device Standards, Ownership and Mobility
 - School and/or Home Usage
 - Integration of Student Owned Devices

Chapter 3 Going Wireless Preparation and Planning

As with most critical decisions, proper planning is of the utmost importance. A WLAN deployment is no different. Not only is the integration of wireless into your district a daunting task, it is one that will make or break the success of your one-to-one initiative. It can also affect your investment in other areas of the technology, including hardware (for laptops), software (operating systems for the laptops or other specific applications), and security (your existing and future network architecture, policies, and with students taking the laptops home, a new level of management requirements).

This section is meant to help you go through the decision making process of procuring, implementing and managing a wireless solution. It is intended to help you identify critical areas to be addressed in your processes of going one-to-one.

The most time and focus of any school district's WLAN project should be invested in the planning stage.

3.1 First Steps

Setting Realistic Goals and Expectations

Goals of a K-12 WLAN

WLANs are most inspiring in the context of what it will be used to accomplish. **How the system will be designed and implemented has everything to do with how it will be used.** A single AP running at 11Mbps begins to see noticeable performance degradation at approximately 10 to 15 simultaneous users. How does this impact the design and eventual success of the WLAN deployment, and ultimately any one-to-one initiative?

The first step is a careful analysis of the intended uses of the wireless technology itself. Take into consideration the applications and uses of the WLAN equipment and architecture over the life of this investment. A typical life cycle of WLAN equipment is three to five years, so having a road map of its intended uses will help you get the most out of this investment. Based on this analysis, a considered plan can be put in place. Once this information is available, an effective site survey can be conducted.

When defining WLAN architecture, focus on two distinct challenges:

- Technology and educational policy requirements; and
- End-user requirements.

Because of increased adoption, more applications and services are being layered onto the WLAN. However, the number of applications utilizing wireless transport is not the only factor that is changing. The characteristics of the applications themselves are changing as well. Traditionally, WLANs in enterprises were intended only for data traffic. The key applications were typical business productivity tools such as e-mail, web browsers, calendaring tools, and messaging. These applications produce network traffic that is irregular and non-continuous. Periods with high network utilization are followed by periods of low network utilization, and the duration of both these periods is unpredictable. The applications load the network in bursts.

It is very likely in the lifespan of this WLAN infrastructure investment that a school district's potential expansion of one-to-one initiatives and/or administration requirements may demand bandwidth-intensive and potentially latency-sensitive applications migrating onto the wireless medium.

Team, Roles and Responsibilities

As with any project plan, identifying the key individuals and clearly outlining the entire team's areas of responsibility is crucial. It is at this stage where the hard skills and actual individual capabilities must be honestly assessed. Ensuring that a district has the in-house capabilities to implement and manage all aspects of a WLAN will be a key to the success of a one-to-one initiative.

Specific one-to-one Initiative Considerations

Identifying which services and applications the WLAN must support is a key to building a robust, relevant, scalable and sustainable architecture. It is strongly urged to consider the following elements of any one-to-one initiative:

- # of students in year 1 through 5 using the WLAN
- Types of application(s) being utilized
- Total bandwidth requirements
- Throughput requirements
- Security for laptops
 - o Special attention should students be taking them home to access the Internet or other resources

3.2 Analysis

**Use a 10:1 and not more than 15:1 Client-to-AP Ratio for your budgeting analysis.
(Client = 1 student laptop or other device to access the WLAN)**

Immediate Scope and Future Scalability

The scope of WLAN deployment is one item that can easily be defined from the start. Whether defined to include all areas of every school in the district, or select classrooms and common areas of a few pilot schools, there is a boundary. Although the scope of your WLAN deployment has a larger impact on the planning and implementation phases, it also plays a role in the architecture.

The architecture must formalize and document the coverage the WLAN provides. The formalization of the scope serves as a guide to ensure neither an under nor over-engineered WLAN solution. Under-engineering provides insufficient resources to the intended degree of service. Examples include inadequate coverage due to not deploying enough APs or failing to incorporate the proper IT security standards at the district level. Over-engineering is the inverse case. This happens when more resources are supplied than are needed to implement the desired solution. In this scenario, there is the potential for underestimating engineering resource allocation, and not meeting the project's financial budget target. An example of over-engineering is deploying too many APs. In this case it results in either overlapping coverage of APs or providing coverage in areas where there is no need for the WLAN access.

A key consideration when determining the scope of your WLAN is how you intend to provide support. You must deal with an increased number of operational issues. Examples include selecting a scalable strategy and platform for managing the WLANs RF, spectrum as well as potentially hundreds of access points and thousands of client devices. Leverage the scope as defined in the WLAN architecture as a planning tool. This structured

approach makes it easier to determine how you offer support at the different levels of the fault resolution path, and how you plan to handle onsite resources for troubleshooting.

One of the key drivers of architecture will be when your district moves to allowing students and staff to bring their own devices, whether laptops, tablets, phones or PDAs and connect to your WLAN. The number of connections must be managed closely, as well as the types, times and priority of applications running over your WLAN infrastructure.

Budget Requirements and Limitations

Budgets are always limiting. Their purpose is to provide a guide on the scope of what can be implemented. It is often times the *unforeseen* elements of many technology solutions that cause the most challenges. This guide, in its entirety, is meant to help identify ALL aspects of implementing wireless into an IT strategy and bring today's best practices to light.

Be sure to include all aspects in a WLAN budget, including but not limited to:

1. Hardware (APs, Controllers, Switches, Laptops, etc.); 2. Software one-time and subscription based charges (WLAN management, Security such as Anti-Virus, Anti-Spam, Anti-Spyware, Network Access Control, Intrusion Detection, Desktop management); 3. Maintenance and Support (in-house and/or out-sourced); 4. Training; and 5. Initial Setup.

Technology Selection

IEEE Standard 802.11 a/b/g/n

Today's Wi-Fi networks operate in one of two frequency ranges: 2.4 GHz and 5.8 GHz. 802.11b and 802.11g operate in the 2.4 GHz realm while 802.11a sticks to the less-used 5.8 GHz band. 802.11b and 802.11g wireless implementations far outnumber 802.11a networks for a number of reasons. First, until 2003, 802.11a suffered from differing regulations for the 5.8 GHz band, making it difficult for manufacturers to sell in some countries. Further, although 802.11a and 802.11g both sport relatively fast speed, 802.11a has a maximum range of 25 meters while 802.11g can range from 25 up to 75 meters, depending on environmental conditions and the WLANs tolerance for slower speeds at the extremities of the coverage area.

While 802.11b and 802.11g support a good distance, the 2.4 GHz range is fairly cluttered and susceptible to interference from cordless phones, microwave ovens and more. Further, this range is also cluttered with other wireless networks, particularly in metropolitan areas. This means that some schools that are close to office buildings or even homes may experience noise from these other WLANs. Each additional WLAN can create an environment that interferes with each other. For these reasons, you may need to maintain 100% control of exactly what authorized devices may connect to the WLAN. Consider rolling out an "802.11a-only" network. Most laptops come with multi-band cards that will simultaneously support 802.11a, b and g, and now even n.

This will be very different for schools located in busy areas, very close to other buildings, office towers and even housing complexes or sub-divisions compared to rural schools that are more isolated.

As identified by Edmonton Public Schools, implementing the frequency which will give you the least interference is likely 802.11a, although with a slightly shorter range, you may achieve more consistent throughput rates. These interference issues are more likely to occur in urban environments.

Hardware Vendor

Overall, vendor selection is one of the many critical steps to a successful WLAN deployment. Each vendor does have varying degrees of competitive differentiation which should be taken into account when procuring wireless solutions. Here are some general categories for assessing the right vendor for any district-wide or individual school implementation:

1. **Product Line:** A vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set. Very simply, select the product that is best suited to the specific environment and requirements.
2. **Financial Analysis:** An assessment of the vendor's overall financial health, the financial and practical success of the business unit and the likelihood of the individual business unit to continue to invest in the product, continue offering the product and advancing the state of the art within the organization's portfolio of products. Note that WLAN vendors range in size from \$10 million to \$100 million to \$90 billion in annual revenue.
3. **Experience and History:** Relationships, products and services/programs that enable customers to be successful with the selected products. Specifically, this includes the way customers receive technical support or account support. This can also include ancillary tools, support programs (and the quality thereof), availability of user groups and service-level agreements. Having implementations and references in the K-12 market is critical.
4. **Future, Scalability and Integration:** It is strongly advised to evaluate vendors on their ability to articulate and envision current and future market direction, innovation, customer needs and competitive forces. Direct, related, complementary and synergistic resources; expertise or capital for investment; consolidation; defensive or pre-emptive purposes related to innovation to ensure a constantly improving solution being offered. For example, a \$100 million and a \$90 billion vendor have dramatically different resources available to grow and address the WLAN business segment.
5. **Simplicity:** A clear, differentiated set of messages consistently communicated throughout the organization from public marketing and advertising information to customer programs. A vendor and their channel partners, who in most cases are the front line of interaction and ongoing communication, should make your buying experience painless and simple. You should never be *talked over* in technical terms.
6. **Depth of Interaction and Relationship:** Vendors use the direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Use a single vendor and centralized management software

This will increase security while optimizing the budget for maintenance and support. For example, with 50 APs on a network, and a security patch for a critical vulnerability is released, it is much easier to push that patch from a management console than it is to connect to individually apply it to each AP.

Implement hardware and software that will be compliant with the up and coming 802.11n to take advantage of the dramatically increased speeds and range, if and when ratified and standardized, planned for the 2008/2009 timeframe.

Dual-Band Radios and Dual Radio Access Points

802.11a/b/g/n multi-band (also referred to as dual-band) APs with two or more radios can simultaneously support both 2.4 GHz (802.11b/g) and 5GHz (802.11a) RF bands (whereas 802.11n can run on either 2.4GHz or 5GHz). They offer backward compatibility (to preserve existing investments) along with a larger number of channels and consequently increased throughput. A wireless station with a multi-band radio typically looks first for an 802.11a AP. If it cannot find one, it then scans for an 802.11g, and ultimately for an 802.11b. Standards for 802.11n are not yet specified.

Multi-band APs are well suited to a wide range of network architectures. Further to the benefits of increased bandwidth, it is common to find deployments that use multi-band APs to segregate data types onto the different RF bands. The APs 802.11a radio can service wireless traffic from data clients (such as student laptops), while the 802.11b/g radio supports more time-sensitive traffic (such as staff and teacher usage) to create two separate RF networks.



Simultaneous 802.11a and 802.11g Dual Radio Support, HP Procurve Networking, Planning a Wireless Network

Alternatively, consider an application in which a multi-radio AP is deployed in a temporary or portable building – for example, in an outdoor portable classroom where there is no Ethernet connection. One radio (and associated antenna) is used for the backhaul link to communicate with a corresponding AP on the main school building, and the second radio (and associated antenna) is used to provide connectivity to users in the local wireless coverage area within the portable.



Wireless Bridging Application, HP Procurve Networking, Planning a Wireless Network

For networks where support for 802.11a is not a requirement, APs may be configured to provide high capacity data. By setting both radios to 802.11g mode, a dual 2.4 GHz radio AP can provide twice the network capacity. This approach is particularly well suited to address areas of dense user coverage, such as adjoining classrooms, large lecture halls or common areas like cafeterias.

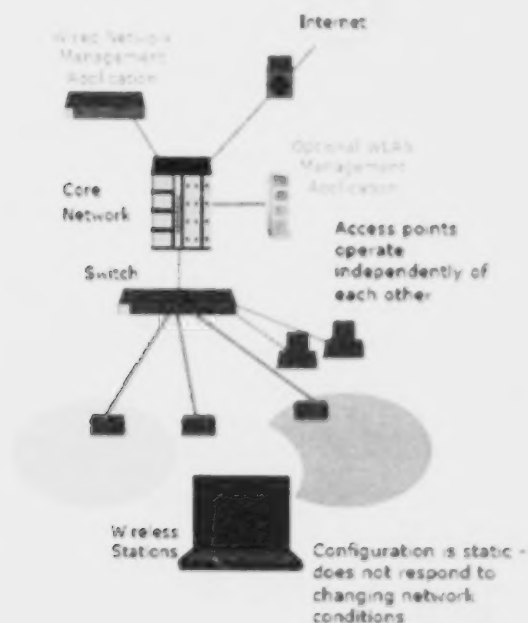
Tip: APs that have at least two radios can be used as a repeater to extend the coverage area.

Centrally Coordinated versus Distributed AP Management

Determine which WLAN architecture to adopt. Both architectures – distributed APs and centrally coordinated APs– have benefits that are well suited to different environments. These architectures are also referred to as *thick* and *thin* respectively.

A wireless network, based on standalone APs, relies on the integrated functionality of each AP to enable wireless services, authentication and security. As shown in Figure 16, this network can be characterized as follows:

- All APs in the network operate independently of each other;
- Encryption and decryption is done at the AP;
- Each AP has its own configuration file;
- Larger networks normally rely on a Centralized Management Platform;
- The network configuration is static and does not respond to changing network conditions such as interfering rogue APs or failures of a neighbouring APs; and
- Be certain to confirm PoE (Power over Ethernet) support, as many *thick* APs do not support PoE.



Wireless Network Consisting of Stand Alone Access Points, HP Procurve Networking, Planning a Wireless Network

In a *coordinated* wireless network, thin APs have much simpler responsibilities. Most of the heavy lifting is performed by a centralized controller, also known as a wireless switch, which handles functions such as roaming, authentication, encryption/decryption, load balancing, RF monitoring, performance monitoring and location services. Because configuration is done once, at the controller, adding additional radios to cover new classroom areas is as simple as plugging them in. As shown in Figure 17, this kind of network can be characterized as follows:

- AP activity is coordinated by a wireless centralized controller. Encryption/decryption and authentication are performed at the controller, instead of at the individual APs;
- To maintain the health of the network, the controller can reconfigure AP parameters as needed, providing a self-healing WLAN (e.g. if an AP fails, neighbouring APs can increase signal strength to make up for the lost coverage of the failing AP);
- The wireless LAN controller performs tasks such as configuration control, fault tolerance and network expansion;
- Redundancy can be provided through redundant controllers in separate locations that can assume control in the event of a switch or controller failure; and
- Supports PoE.



A Centrally Controlled Wireless Network, HP Procurve Networking, Planning a Wireless Network

Both the distributed and centrally coordinated architectures have advantages and disadvantages, depending on the age of the wired infrastructure, deployment area, building architecture and types of applications to support. Regardless which approach, it is essential that the architecture provides a way to manage the WLAN efficiently and effectively.

A *distributed AP WLAN* is particularly well suited in environments where:

- There is a smaller, isolated wireless coverage area that requires only one or a few APs; and
- There is a need for wireless bridging from a main building to a remote portable or temporary building such as a portable classroom.

However, the operational overhead to manage and maintain a WLAN increases with the size of the WLAN deployment. Wireless LAN management tools that are generally proprietary to each vendor's associated hardware help simplify configuration and monitoring of the LAN, but the inherent "independence" of these APs presents a challenge in addressing security, configuration control, bandwidth predictability and reliability.

It is worth noting that when APs are first deployed, they must be configured. Such things as radio settings and authorized users must be added. Once WLANs are installed they are subject to frequent change as manufacturers update firmware and introduce new products; as new students are introduced and as security codes are updated. Each of these changes requires an administrator to "touch"—physically or electronically—each AP or device that connects to the WLAN. It is not cost effective to manage WLANs device by device, and hence if there will be more than just a few APs on your WLAN, opt for the centrally coordinated architecture.

A centrally coordinated WLAN is well suited to deployments where:

- There are one or more large wireless coverage areas that require multiple APs possibly accompanied by several smaller isolated coverage areas;
- RF network self-healing is required; and
- A redundant stateful-failover solution is required.

There is no question that the trends indicate centrally coordinated solutions are becoming the de facto standard. As wireless LAN deployments continue to grow larger, accommodating ever greater numbers of users, there will be an increasing demand to centrally manage a wide range of security, performance and configuration attributes as a single system from a single dashboard or software interface.

A centrally coordinated network offers many benefits, including:

- Lower operational costs. Centralized management facilitates ease of deployment and ongoing management. It is essential to minimize help desk calls and trouble tickets.
- Greater availability. In this architecture, it is easier to respond in real-time to changes in the network performance and spikes in user demand such as new students or temporary staff.
- Better return on investment. Fast client roaming and enhancements in Quality of Service provide traffic-sensitive applications with their required throughput.

As for all of their attractions in terms of performance, flexibility and affordability, WLANs also pose management challenges very different from those of wired networks. These challenges increase geometrically as WLANs grow in size, scope and complexity. The solution is to automate these management tasks by implementing best practice service level management processes and tools.

Emerging field tools are also complementing IT toolkits in filling the need to effectively manage the wireless environments. These tools provide the ability to detect rogue APs, determine security levels, determine where there are potential interference sources for wireless, such as cordless phones, and analyze wireless data.

There are many different ways to set up a wireless network. A certain density of APs is required to provide satisfactory network coverage and capacity, while many aspects of WLANs are analogous to wired LANs and should be managed in a consistent fashion, some aspects of wireless are unique. Wireless is a shared medium and, as such, requires careful planning for dynamic usage profiles and capacity variations.

Antennae Selection

Antennae allow for more efficient coverage for specific areas, and can help achieve desired coverage, capacity and bandwidth objectives. A higher-gain antenna focuses the radio's RF energy into a smaller area to achieve higher signal levels and a better SNR (Signal to Noise Ratio). This typically yields higher data rates over the area covered by the antenna.

For example, a library with floor-to-ceiling solid wood or metal bookshelves, and wireless network access of PDAs or laptops is required within this area, deployment of external directional antennae to focus wireless coverage between each of these obstacles would be required.

Antennae and Cabling

In very small networks, the retail box store, consumer-grade, wireless router with its default antenna is generally adequate. However, as a wireless network grows beyond a confined area, antenna choice becomes more important. Every different kind of antenna emits a unique radiation pattern, making certain antennae more suitable than others for specific applications. For example, a point-to-point wireless network connecting two buildings will usually not use the small omni-directional antennae shipping with most APs. Instead, specialized antennae that focus the transmission signal are used in order to achieve higher throughput and, sometimes, to lessen the scatter associated with less focused antennae. There are a large number of different types of antennae available for use with wireless networks. When considering antennae, also be mindful of the cables that connect antennae to your AP. The word “wireless” is a bit misleading. In reality, wireless APs typically need at least one cable—a Ethernet cable—in order to function, excluding APs configured as repeaters. However, if an AP configured as a repeater without a Ethernet cable still requires power but would not have the possibility of leveraging PoE, hence it would need to be physically wired for power. Beyond repeaters, if APs do not support Power over Ethernet (PoE), you also need to plan for power outlets at each AP location.

This is one prime difference between the consumer-grade AP and the more expensive units designed for business, education and enterprise environments. The more expensive units generally support PoE. In addition to the network cable, be mindful of how much cabling is used to connect an AP to an external antenna. The longer cable, the more loss introduced in the transmission, resulting in lower throughput and fewer supported users per AP.

Antennae Types

Four main types of antennae are commonly used in 802.11 wireless networking applications: Parabolic Grid, Yagi, Dipole, and Vertical. For more detailed information on antennae, refer to http://www.hp.com/rnd/pdfs/antenna_tech_brief.pdf.

Each is described in detail as follows:

Parabolic Grid

Perhaps the most powerful antenna for site-to-site applications is the parabolic grid antenna. A parabolic grid antenna can take many forms, ranging from something that looks like a satellite TV dish to one that has the same shape but is made of a wire grid instead of having a solid central core. This type of antenna is a unidirectional antenna, meaning that it transmits only in the direction in which the antenna is pointing.

Yagi

A yagi antenna is slightly less powerful than a parabolic grid, and it is suitable for site-to-site applications at lesser distances than a parabolic grid antenna. Like the parabolic grid, the yagi is also a unidirectional unit. A yagi antenna consists of a series of metal spokes radiating from a central core. The whole thing is covered by a tubular plastic housing called a radome, often concealing the actual antenna elements.

Dipole

A dipole is a bidirectional antenna, and its radiation pattern extends in two directions outward. It generally consists of a base with two antenna spokes going in opposite directions. Use a dipole antenna to support client connections rather than site-to-site applications.

Vertical

A vertical antenna is exactly what it sounds like – an antenna that sticks in the air. A vertical antenna's radiation pattern extends in all directions from the unit, losing power as the distance increases. Like the dipole, a vertical antenna's primary use is for client support. Most wireless APs come with a small vertical antenna. A vertical antenna is omni-directional, meaning that the signal radiates in all directions.

Antenna specifications

Understanding the different antenna types is only the beginning. Each antenna type has a number of specifications that directly affect how well it works. These specifications are antenna gain, beam width, loss, and radiation pattern.

Antenna gain

This is a measurement of how well the antenna focuses a signal. This is typically measured in dBi (decibels relative to isotropic radiator—a theoretically “perfect” antenna) and is based on decibels, which is a logarithmic measure of relative power. The dBi is computed by comparing the output of the antenna to a theoretical isotropic radiator (antenna) with a dBi of 0: the higher the dBi measurement, the higher the power level of the antenna.

Beam width

The beam width is the area radiating outward from the antenna where the signal within a specific angular distance is above the “half power” of the peak intensity of the antenna. The beam width is also loosely used to determine the antenna type. A parabolic grid antenna is a unidirectional antenna with a very low beam width, which means that it needs to be very carefully aimed at its partner in order to be effective. A vertical, omni-directional antenna has a very high horizontal beam width, which is why it is suitable for roaming client connections. However, its vertical beam width will be lower. In general, there is an inverse correlation between beam width and antenna gain, which means that the required accuracy for aligning antenna goes up as the gain increases because the beam width decreases.

Loss

Loss is an important factor when deploying a wireless network, especially at higher power levels. Loss occurs as a result of the signal traveling between the wireless AP and the antenna. Since APs are typically connected by a cable, there will always be loss. You can minimize loss by using the appropriate type of cable in the minimum length required to make the connection.

Radiation pattern

Every antenna has a unique radiation pattern determined by its construction. This radiation pattern is a three-dimensional radiation field of the antenna’s output. Some manufacturer’s antenna supply sample radiation pattern specifications for their equipment. You can use these specifications to determine how far the signal from a particular antenna can travel before becoming unusable. As a rule of thumb, a directional antenna has a conical pattern of coverage that radiates in the direction that the antenna is pointed, while an omni-directional antenna’s area of coverage is shaped like a doughnut.

3.3 Project Plan

Timeframe

A modest estimate for a technically competent team of technicians to plan, communicate, survey, procure, configure, secure, test and report on a basic WLAN implementation (e.g. one school site with up to twenty APs) ranges from one to three calendar months. In Table 6 below is a sample project plan timeframe. This timeline can be adjusted (either shorter or longer) depending on the overall scope, size of the project team and the number of personnel involved in decision making.

Table 6 - Sample WLAN Project Plan, Network Integrators of Canada Inc.

Sample WLAN Project Plan			
Step	Plan and Communicate	# of Days	Running Total Time in Days
1.00	Determine the scope including the number of schools, size of the required coverage area(s), number of users and one-to-one initiatives to be supported.	2	2
1.01	Set goals and expectations.	0	2
1.02	Define roles of project team members.	1	3
1.03	Define budget	1	4
1.04	Draft mid to long-term plans (1-5 years) to allow for scalability in line with strategic business planning	1	5
1.05	Decide on wireless encryption and authentication protocol	1	6
1.06	Determine minimum security requirements	1	7
1.07	Identify compatibility and/or required upgrades and configuration changes to existing hardware, software, network architecture and maintenance/support structure (e.g. Authentication server, Internet connectivity, backbone switching architecture, NICs, VLAN supporting firewalls, etc.)	4	11
1.08	Outline usage and applications to be run on the WLAN to estimate additional bandwidth, speed and latency requirements	2	13
1.09	Select target client:AP ratio, approximate cost per AP and percentage of AP to total budget (e.g. 10:1, \$250 and 20%)	0	13
	Sub-Total	13	13
Site Survey			
2.00	Obtain floor plans for all schools included in the project	3	16
2.01	Determine how many APs it will take to provide a signal to the desired coverage area	1	17
2.02	Physical AP placement map	1	18
2.03	Identify signal trouble areas and physical construction or environmental challenges	0	18
2.04	Determine user policies for the wireless network	1	19
2.05	Diagram channel layout of APs	1	20
2.06	Confirm hardware compatibility (include desired legacy hardware, new hardware and current or future for student owned device standards)	2	22
2.07	Verify that each APs location is physically secure	0	22
2.08	Verify that there is a power source near the intended location for each AP or PoE compatibility	1	23
2.09	Confirm there is a way to run a patch cable between your wired network and each AP and/or APs to be used as repeaters. List specialized antennae requirements	1	24
2.10	Determine AP network cabling distances and are within CAT-5 or 6 limits (~100m)	1	25
	Sub-Total	12	25
Procure Hardware, Software, Services and Training			

3.00	Research and review vendor WLAN solutions	3	28
3.01	Meet top two to three WLAN vendors for face-to-face presentations on their solutions	5	33
3.02	Purchase infrastructure upgrades identified in planning stage (e.g. District head office and/or school site WAN speed increase from 10Mbps to 60Mbps and switch upgrades from 100Mbps to 1Gbps)	21	54
3.03	Buy the necessary AP, Controllers, Management software, and wireless NICs	5	59
3.04	Record the MAC address of all hardware	1	
3.05	Purchase other upgrades identified in planning stage	5	64
3.06	Record and distribute all vendor and out-sourced service company or VAR technical support contact information to Implementation team	1	65
3.07	Register with all vendors using a centralized and common email address for alerts, support notifications, etc. (e.g. WLAN@yourdomain.com which is aliased to all relevant members)	1	66
	Sub-Total	42	66
	WLAN Implementation and Security		
4.00	Configure and install WLAN controller	1	67
4.01	Install a pilot set of APs at one location	1	68
4.02	Configure clients (e.g. Standard setup for a one-to-one laptop)	1	69
4.03	Test and fine tune client:AP ratio	1	70
4.04	Adjust AP and antennae placement	1	71
4.05	Roll-out all APs at all locations	3	74
4.06	Record physical location of all hardware (by MAC addresses), use floor plans	1	75
4.07	Configure remaining clients	1	76
4.08	Test and Fine tune all	3	79
4.09	Configure and implement security settings for VPN, VLAN, NAC and/or other hardware and software (advised to perform on pilot area, test, then roll-out)	5	84
4.10	Vendor product training on Controller management software. Reset all passwords to high level of entropy, get familiar with interface, features, capabilities and reports	3	87
	Sub-Total	21	87
	Assess project and repeat above steps as necessary	10	97
	Integrate WLAN into IT strategy and maintenance and support structure	10	107

Scope

Ultimately, the scope is defined by budget.

$$\{ 10 \times 10 \} \neq 100$$

Ten schools with ten APs each is not the same scope as one school with one hundred APs

A common pitfall with implementation of wireless solutions is missing the hard costs associated with a total solution. For example, simply spending 100% of the budget on mobile devices would not be a solution. In the same light, allocating the entire budget for just APs and laptops still is not a viable solution.

So what are the inter-related elements to be considered to find the optimal balance and achieve maximum coverage and quality of experience for the wireless users, students and staff. The following matrix will assist with

identifying 25 key elements that are all factors to be considered in a WLAN implementation in a K-12 school district. There are many more, however, and filling in these 25 will direct the appropriate resources, timelines, policies and solutions into place.

Table 7 - WLAN Scope Elements, Network Integrators of Canada Inc.

Key Inter-Related Elements of Scoping a WLAN Implementation: Optimization Matrix

APs: Thin or Thick	Existing Internet Pipe at School Site	Traffic Topology	Desktop Management	Time
Controllers	Existing Internet Pipe at District Head Office	Client:AP Ratio	Compliance (NAC)	# of School Sites
# of Laptops	Security Tolerance	IT Staff	Standardized vs. Non-Standardized Clients	Budget
# of Student WLAN Users	Existing Network Hardware	Out-Sourced IT Service Partner	Scalability	Usage Policy
Application Types	Coverage Area	WLAN Vendor	Life Cycle	Ongoing Support Requirements

Client-to-AP Ratio

Many different factors impact the performance of your WLAN such as:

Internal Factors:

- The shared nature of the communication medium;
- The access mechanism for the medium;
- The use of a limited number of communications channels; and
- The available bandwidth.

External Factors:

- The number of users;
- The types of devices communicating across the WLAN;
- The types of applications used on the network; and
- The degree of mobility that is demanded by the user community.

Knowing the traffic types and usage patterns on the WLAN is fundamental to designing a solution that not only performs correctly, but also delivers a relatively consistent level of service. As such, providing the WLAN with the proper number of APs is a contributing factor to creating a WLAN that meets a performance baseline. The simple translation is that determining and managing the number of simultaneous connections will be critical to controlling a WLAN environment.

A non-technical solution may be to schedule classes at different times to use the same APs, and hence maintain a tight budget. Another alternative, more to address performance issues over budget would be to not situate classes utilizing the WLAN in adjacent rooms. Having one-to-one classes located in opposite ends of the school, or at least far enough away to be exclusively accessing a different set of APs would do the trick.

The industry has converged on the metric "client-to-access point ratio" to denote the number of users a single access point can consistently support. However, do not take the term "client" at face value. Indeed, a student that uses the WLAN primarily for e-mail and web browsing will have different bandwidth requirements than a

student using Computer Aided Design (CAD) programs using the WLAN mainly for streaming intensive applications. As such, carefully consider the types of clients and their respective network needs, such as bandwidth and throughput requirements.

Do not make the assumption that more senior students will be utilizing more intensive applications either. Primary students' applications may likely be more graphical or interactive, and high school students may well be utilizing simple file access for documents and less intensive applications.

The client-to-AP ratio is expressed as a number such as 10:1, and not more than 15:1. In this case, the number 10 or 15 represents the recommended maximum number of clients that can be associated to an AP at any given time.

Exceeding this ratio will degrade the expected performance. Three different strategies can be used to determine what an environment's optimal client-to-AP ratio is. Benchmark tests to identify exactly what works, classify users and traffic types to generate more granular client-to-AP ratio specifications, or simply adopt client-to-AP ratio guidelines that have been published by most vendors. Each strategy has its merits and drawbacks.

Benchmarking enables the most precise identification of the client-to-AP ratio. Local variations are measured and the ratio can be optimized depending on the exact user profiles and needs. However, not only is this approach time and resource intensive, but it also creates a dated snapshot. If the environment changes, for example, and adjacent classes running simultaneously introduce new software with different traffic signatures, the benchmarks will no longer be accurate.

By classifying both traffic and users, some degree of customization can be captured. The process is relatively straightforward and can be performed by your network architects and designers. A challenge that you will likely face with this method is the identification of the correct segmentation of the users and traffic types. Do not reinvent the wheel. Follow the classification guidelines as set forth in your architecture. Given the benefits of more accurately identifying a client-to-AP ratio that yields a more consistent and satisfactory WLAN user experience, this approach is recommended.

The final strategy is to accept the recommended client-to-AP ratio as published by the WLAN equipment vendor. Even though this is the easiest solution, there is potential for over- or under-provisioning the number of APs because the information provided by the vendor does not consider your specific user-base requirements. However, use the WLAN vendor's published recommendations as a rough guideline.

3.4 Technical Deployment Considerations

Network

Compatibility Overview

Some key points to be considered are:

- Wireless access and authentication is hardware specific;
- Older wireless cards will not support WPA2. Computer upgrades may be required to meet security policies;
- If using thick APs, use all the same brand and model for ease of configuration and management; and
- Configuration files can be pushed out to clients if they are standardized.

A factor that affects scalability is compatibility, and this is a two-pronged consideration – compatibility of wireless technologies with one another and compatibility with wireless devices, especially the network adapters built into many of today's laptop computers. A big advantage of 802.11g over 802.11a is its backward compatibility with 802.11b. This means that starting small with an inexpensive 802.11b AP and then later replace it with an AP that supports both b and g. Computers that have 802.11b network adapters will still work, but at the lower 802.11b speeds. Replacing NICs gradually makes for a smooth transition. Switching to 802.11a, everything will have to be replaced immediately because it is not backwardly compatible with old 802.11b equipment.

Another challenge with 802.11a is that 802.11b or g built-in wireless equipment in laptops is more common. These will be useless with an 802.11a infrastructure.

Finally, staff or students who connect may also want or be required (if taking laptops home for homework and assignments) to connect to other wireless networks at their homes or at public access points (hot spots). Most home and public wireless networks use 802.11b technology. Implementing a standardized policy for school owned laptops used by students in a one-to-one program is highly recommended (see Chapter 7 on Technology Management).

Architecture

Things to consider when determining network architecture include:

- Backbone inter-connect speeds at individual school sites and/or (if hub and spoke design) at district head office site, may need upgrading to support new users;
- VLANs: is there capacity for more to segment the WLAN;
- Firewall policies and restrictions: e.g. block the AP to WLAN Controller traffic; and
- VPN capacity. Checking actual VPN throughput is recommended.

Security

Although wireless networking can make learning more enjoyable for students, it can also become a massive security challenge if not setup and managed appropriately. As such, it is important to have an effective wireless networking policy in place across the district's network.

A big security challenge with wireless networks is that they transmit potentially sensitive information over the airwaves. This means that the information flowing across the network can be intercepted by anyone within range who has a laptop equipped with a wireless network card. Likewise, wireless access points provide a way for hackers to enter your network without having to deal with the constraints normally associated with an Internet based attack. As such, wireless networks can pose a huge threat to your network's security unless you have a good wireless network security policy in place coupled with the latest security technology (e.g. WPA2 with EAP, see Chapter 4 on Security).

Matching Your Policy to Your Administration Model

The administrative policy should be a document that specifies how wireless hardware will be connected to the wired network, and by what type of user. This is critical because, as with many of districts, the IT department is decentralized with technicians working at various locations including their home, school sites and the district office. Be sure to select one standard encryption methodology for all schools within the district. Employ a top-down approach and ensure this decision is implemented at all school sites.

Develop a strong and encompassing wireless networking policy. One clause strongly recommended is that wireless APs must only be attached to a dedicated network segment, and not to a segment containing other network resources.

Hardware

Points to consider include:

- May require switch upgrades to support PoE, VLANs or capacity;
- Older hardware is incompatible with new security standards; and
- Can older hardware support the new wireless cards? Is there room for them?

Software

Application characteristics must be analyzed if this traffic is to flow over the WLAN. It is essential to outline this in the policy to protect and ensure scalability as planned.

Performance is not limited to the throughput that a client can achieve. It is also directly related to the client keeping its network connection and communication session intact. When roaming from one AP to another, there is a small amount of time during either authentication or association during which the client will effectively be without a link. The duration of the lost link will determine if and how applications will be impacted. Note that fast roaming was specifically conceived to make this link loss during authentication almost unnoticeable to end users.

Applications exhibit a distinctive sensitivity to the duration of a lost link. Transactional applications such as e-mail and web browsing are relatively insensitive, whereas real-time applications such as voice and video are highly sensitive. Ensure that fast roaming is enabled to make authentication occur promptly enough to not affect the core WLAN application suite.

Application bandwidth requirements can be analyzed by the software vendor's specification or manuals. A common issue with networked applications is that they are developed with little or no consideration for the resources they require from the communications infrastructure. Application developers take into consideration the notion of the network, but typically fail to consider bandwidth and latency implications. The (false) assumption is that the network is always available, that bandwidth is unlimited and that congestion and delays do not occur. As such, even though the applications and the network are tightly coupled, they are typically developed and deployed as independent components. It is exactly this decoupling that creates the burden of carefully planning a WLAN for successful support of the extension of applications to the wireless environment. Hence, start with the premise that the average application is not aware of the transport medium it is using. They treat the network—wired or wireless—identically.

The challenge of applications not being aware the network is compounded with WLANs. Indeed, most applications are developed for wired environments, however, they will likely be developed specifically for the one-to-one initiatives in the education sector. Specific characteristics of WLANs are their lower throughput and higher latency than their wired equivalents. This is typically not a problem for the bursty applications. However, WLANs

can cause additional challenges for applications that demand high data rates or deterministic behaviour. The interaction between applications and the network is only one of the challenges that must be tackled when defining WLAN architecture. Defining a wireless architecture to support voice and video also introduces specific problems that must be considered. The considerations include provisioning sufficient bandwidth for latency-sensitive applications, implementing a quality of service (QoS) solution, and ensuring fast-roaming capabilities between cells.

Perhaps today's students will be in one classroom and it is unlikely that they will be roaming between APs, which sounds like a rational and fair statement. However, recall that this WLAN investment is meant to last districts up to five years. In the world of technology, five years is a very long time, and it may very well be that a district will want to implement other applications and devices to run over the WLAN. One such example, which could be used by students or more likely teachers, is that of Voice over WLAN handsets.

Speed requirements

Speed and distance can be important factors in scalability of a WLAN. As schools integrate more and more technology into the learning process, policy changes such as students bringing their own devices onto WLANs will add more and more users. In addition, more bandwidth will be required for the transfer of larger files and for higher bandwidth technologies such as streaming audio/video, real-time conferencing and so on. That means the more bandwidth, the better.

802.11a and 802.11g provide more scalability in this regard than 802.11b and 802.11a can combine channels to get even higher throughput. Distance range can also be a factor in the scalability. Should a school site expand physically, more APs to reach the areas with 802.11a would be required than with 802.11b or g.

802.11n is hoping to solve much of this area's frustration, however is not yet available in the marketplace.

Ensuring that all of your solution is compatible with 802.11n will provide scalability to higher speeds down the road.

Alberta SuperNet

Alberta SuperNet is a fibre-based broadband network that links over 4200 public sector sites in 429 communities across the province. These sites include schools, post-secondary institutions, hospitals, libraries and municipal and government offices. The network was commissioned in 2000 and the initial rollout was completed in Fall 2005.

Currently, all publicly funded school jurisdictions in Alberta have wide area network (WAN) connections using Alberta SuperNet. This broadband network allows these districts to centralize many IT services and supports. This can include the centralized support for WLAN installations at multiple sites. At present, the maximum bandwidth available for a network head-end connection is 60 Mbps. Gigabit Ethernet services allowing much higher speeds (up to 800 Mbps) should be available to SuperNet customers by late Fall 2007.

See Chapter 8, Calgary Public Case Study.

Site Survey

A site survey identifies the optimum locations for APs, given the access and bandwidth requirements outlined by the plan and design. An important note to make here is that a quality site survey is much more than a simple physical walk-through of a school. An experienced network technician will use a combination of specialized electronic tools, practical experience and specific floor plans showing the locations of one-to-one learning

environments. An effective site survey should indicate how many devices should be able to use the intended applications concurrently, and at what locations within a school building or buildings they can support.

When the survey is done, a report should be developed which includes:

1. A summary statement on how the WLAN is to be used and what it is intended to achieve including the audiences and applications. Try to project this for more than just the current year's one-to-one plans. Ideally, at least a three-year road map would be useful.
2. An analysis of the physical structure and its fitness for wireless resources.
3. Reports of the data resulting from the tools for predicting the likelihood of success of a wireless implementation and the optimum placement of APs. These tools can predict possible problems with high demand, coverage conflicts and overlaps, dead spots, etc. This should include the number of APs needed.
4. Because the rule of thumb is a maximum of 10 to 15 simultaneous users per AP (e.g. using 802.11b), the report should predict the current ratio of users to APs.
5. A map of the preferred placement of APs based on the site survey. This should also include information on the anticipated configuration of each AP for use in management and security of the WLAN environment including 802.11 a, b, or g channel selections. Some of the more obvious configuration items are the name and channel of the AP, the coverage area, authentication and encryption type, IP addresses and MAC addresses (to be entered upon procurement of hardware).
6. Identify neighbouring APs and WLANs
7. List desired coverage area(s). Identify any odd-shaped buildings, corridors, aisles, and similar limitations that might affect the placement and/or number of APs and antennae. Through proper selection and placement of antennae, you can extend coverage into desired areas, overcoming physical obstacles and multipath interference.
8. Signal characteristics throughout the coverage area including strength, signal-to-noise ratio (SNR) and *packet retry count* (the number of times packets were retransmitted for successful reception).

The magic number for packet retry count is 10 percent. There should be no more than 10 percent in any area. Use packet retry in tandem with the SNR reading for a good picture of signal quality. The signal might be strong enough, but because of noise or multipath interference, packets are resent. Without an SNR reading, you cannot tell if packet retries spike because you are out of range, there is too much noise, or the signal is too low.

See the Implementation Chapter's WLAN Performance Testing section for further information on this and a sample list of vendors.

AP Location for Site Survey

When performing a site survey, situate the APs as close to their final mounting positions as possible. This helps resolve any problems that might creep up after mounting the AP. In most cases, APs should be mounted at ceiling height. In areas with high ceilings, take advantage and mount them between 15 and 25 feet as this will help to account for large influxes of physical student body traffic. If mounted at this height, power delivered to the devices must be addressed. PoE is optimal to avoid time and cost associated with electrical outlet installation. PoE can save a lot of headache and expense.

Physical Security

Although vandalism has not been identified as an issue with any of the districts interviewed, in less frequently monitored areas, it might be desirable to keep the AP out of sight and reach. If the AP is placed above ceiling panels, antennae should still be placed below the panels for optimal reception. If this is the case, purchase an AP

that fits for remote antenna capability and do not put the antennae unnecessarily far away from the AP as there will be increasing signal loss.

Check your local building and fire codes. You might need plenum-rated APs and cabling if they are placed above the ceiling tiles in open air return systems.

Signal Strength

In general, objects absorb or reflect signal strength and degrade or block the signal. Identify any potential obstacles or impediments in the area to be served. Examples of common objects that a school's WLAN may encounter are:

Walls – especially if the wall is composed of heavier construction materials, such as concrete. Also note any firewalls (physical construction firewalls, not the electronic kind) in the area.

Ceiling tiles – particularly if they are made of material such as metal.

Student Body – For example when the bell rings and a wave of bodies flood the corridors, a dramatic loss of can occur during these times.

Furniture – especially pieces that are primarily made of metal.

Natural elements – such as water, trees, and bushes – not only outdoors, but also in many courtyards or other interior public spaces.

Wood floors – can allow floor-to-floor interaction between APs causing channel interference or other noise. Think three dimensionally.

Classroom doors – these should be closed before beginning the survey. This shows how the WLAN performs in real, day-to-day functioning, so that is how it should be surveyed.

Coated glass – transparent glass generally does not greatly degrade signal strength. But it may do so if it is coated with a metallic film or has a wire mesh embedded in it.

Cell Layout and Channel Usage

Most scenarios require more than two APs to cover the appropriate area within a school. Therefore, you need to consider the layout and configuration of more and more APs to scale the design to fit the wireless environment.

For example, to cover the entire area of a wing of a school or one floor of the entire building, APs must be placed at regular intervals throughout that space. Information from the site survey is vital toward deciding on final AP placement, as actual live measurements can be used with an AP staged at various points in the actual space.

The two basic elements of designing a WLAN are:

- Sizing the AP cells; and
- Selecting channels for the AP cells.

Sizing AP Cells

The size of AP cells determines the number of APs that must be purchased and deployed to cover an area. However, the design should not be driven by cost alone. AP cell size can also affect the performance of the APs

as clients move around or gather in one place. Within a single AP cell, all the clients associated with that AP must share the bandwidth and contend for access. If the cell is large, a large number of clients could potentially gather and use that AP. If the cell size is reduced, the number of simultaneous clients can also be reduced thus offering higher throughput potential.

Large cells can allow clients to step their data rates down as they move farther away from the APs. For example, when an 802.11b client is near an AP, it can use the highest data rate (11 Mbps). As the client moves out away from the AP, the data rate can be reduced to 5.5, 2, and finally 1 Mbps. Clients may need to use only the highest data rates in a cell, which can be accomplished by reducing the cell size.

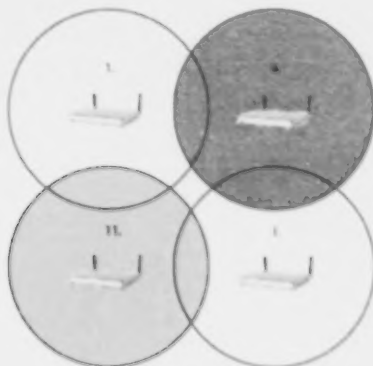
Generally, the AP cell size is driven by the APs transmit power. Higher power equates to greater range, so the power must be adjusted so that the APs signal does not propagate into nearby AP cells operating on the same channel, which should be dramatically minimized with an efficient layout plan. Once the AP cells have been sized and pinpointed, clients should be able to associate and roam at any location within the coverage area.

No clear rule of thumb exists for sizing AP cells for a specific number of clients. As with switched networks, the limiting factor is the demand of client's applications and the simultaneous volume of data moving over the medium.

As a very loose guideline, consider the maximum peak throughput of a wireless cell divided by the number of simultaneous clients to determine a maximum data rate per user. Factoring in the overhead of 802.11 encapsulation and bandwidth contention, 802.11b can offer around 5 Mbps through each AP, whereas 802.11g and 802.11a offer up to 23 Mbps. This means, for example, in an 802.11b cell with 25 clients, each client would have a maximum throughput of $5 \text{ Mbps} / 25$, or 200 Kbps. In an 802.11a or 802.11g cell, those same 25 users would have $23 \text{ Mbps} / 25$, or about 1 Mbps.

WLAN Channel Layout

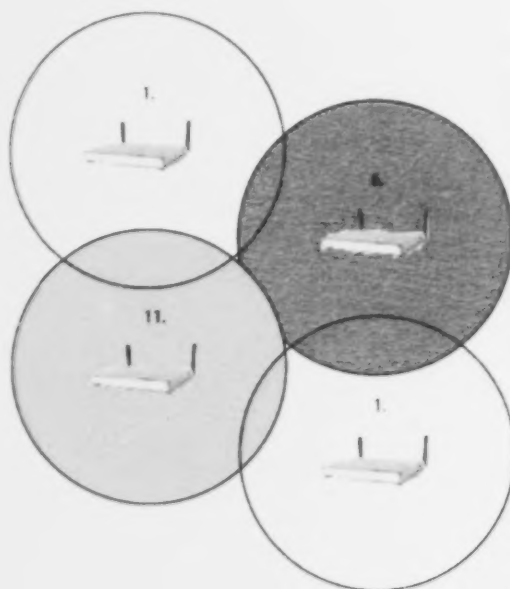
To minimize channel overlap and interference, AP cells should be designed so that adjacent APs use different channels. 802.11b and 802.11g limit using channels 1, 6, and 11. The cells could be laid out in a regular, alternating pattern, as the following Figure 18 illustrates.



Alternating Channels, Network Integrators of Canada Inc.

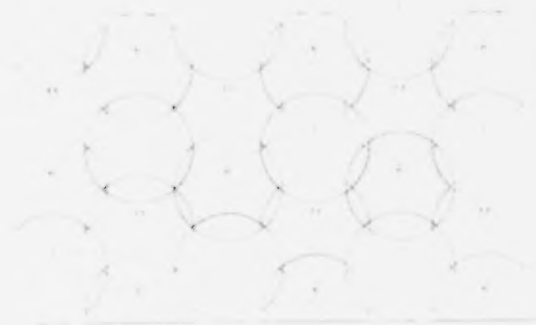
However, notice the very center where the cells meet, there is a small hole in RF coverage. This may not be a significant problem depending on the required layout of coverage area, however any hole can pose a problem if a client roams through the area, his wireless signal will probably drop completely. As well, it cannot be solved properly even if the cells were brought closer together to close this hole, as the two cells using channel 1 would overlap and begin interfering with each other.

The solution is to lay out the cells in a honeycomb fashion as illustrated below. The honeycomb pattern is seamless, with no holes. As well, the cells using the same channels are well separated, providing isolation from interference and unlimited scalability in design. As far as ordering channels in the pattern, several different variations are available using combinations of the three channels.



Alternating Channel Pattern, Network Integrators of Canada Inc.

Notice that as the client shown in the channel 1 cell moves around, it will roam into adjacent cells and change channels. In order for roaming to work as it is intended, a client must be able to move from one channel into a completely different channel. Alternating channels is referred to as channel reuse. The basic pattern shown in the previous figure can be continually repeated to expand over the required coverage area, as the next figure illustrates.



These examples have been illustrated with Fig. 11's setup. If a user compares with Fig. 11a due to the larger number of channels against the user. However, the design is also different. Fig. 11a can also be kept as even though with overlapping channels, so channels of adjacent users along the same channel is much lower.

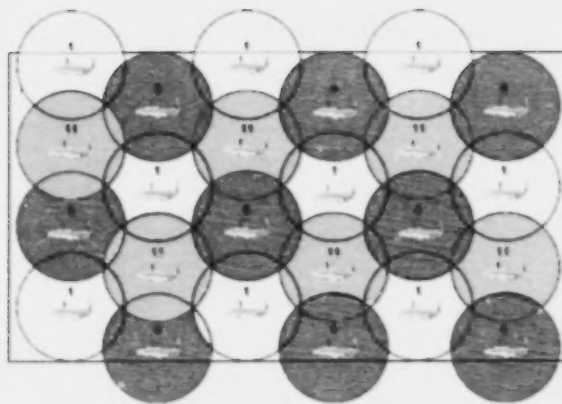
So far, only two-dimensional coverage has been considered. If a user has the first two dimensions of the coverage area, a three-dimensional design must be implemented.

Recall that an RF signal propagates from an antenna takes a 3D space, from the origin. As shown in the Antenna section, an omnidirectional antenna coverage pattern is illustrated with the antenna base. In the field, compared to omnidirectional pattern, the antenna is not always in the direction of the antenna is pointing.

The following examples are a three-dimensional pattern. The omnidirectional pattern is a circular shape, and the pattern in the field and coverage pattern of the AP are also shown there.

Two channels of adjacent users would be staggered from the user and shown in the next section.





Channel Reuse, Network Integrators of Canada Inc.

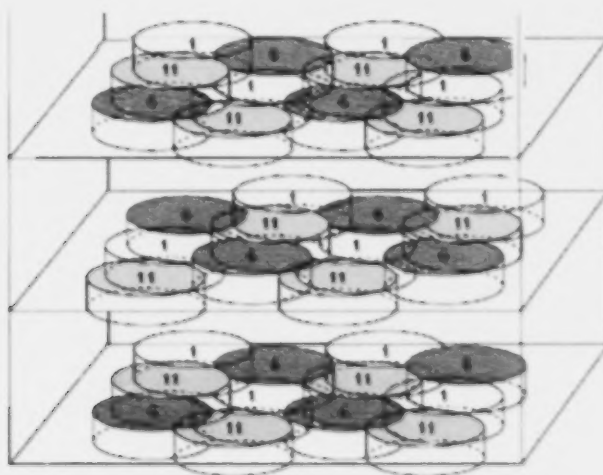
These examples have been illustrated with 802.11b/g setups. It is even simpler with 802.11a due to the larger number of channels available for use. However, the design is quite different. 802.11a can utilize four, eight, or even twelve non-overlapping channels, so chances of adjacent cells using the same channel is much lower.

So far, only two-dimensional scenarios have been assessed, but should more than one floor be included in the coverage area, a three-dimensional design must be implemented.

Recall that an RF signal propagating from an antenna takes on a three-dimensional shape. As outlined in the Antennae section, an omni-directional antenna's coverage pattern is donut shaped (with the antenna being in the middle) compared to unidirectional which appear as more cone shaped in the direction the antenna is pointing.

The following example uses omni-directional antennae. The antenna signal extends outward, giving the cell a circular shape above and below on the floor and ceiling, possibly affecting AP cells on adjacent floors.

Cell channels on adjacent floors should be staggered both beside and between floors as presented below.



Channel Reuse across multiple floors, Network Integrators of Canada Inc.

Alternate channels adjacent to one another on the same floor, and between floors for a non-overlapping design. Channel 1 on the second floor should not overlap with channel 1 directly above it on the third floor or below it on the first. The cell size, AP transmit power, and channel assignment all have to be coordinated on each and every AP. Roaming also becomes challenging if clients are permitted to roam across the entire school's wireless network.

Point-to-Point Bridging

This would take place where it is not feasible to run a network cable between two buildings to join their respective LANs into a single Layer 3 broadcast domain or due to budget limitations whereby wireless repeaters are cheaper than a hard wired solution. If the two buildings are a reasonable distance apart and ideally in direct line of sight with each other, wireless bridges can be configured. In this mode, wireless APs are configured to forward traffic between each other and not act as wireless APs for client access.

Noise and Interference

Noise from cordless phones, wireless headsets, Bluetooth devices and other non-protocol devices can interfere with an AP trying to send or receive data. The site survey should identify sources of signal noise present in each deployment area so that the WLAN can avoid at least the already existing noise sources, or remove the sources of noise.

Consider the following four common misconceptions surrounding noise and interference for WLANs:

Misconception 1: "WLAN hardware addresses interference automatically."

Most centrally coordinated wireless controllers, or smart switches, do manage RF interference problems, however, they are limited. In response to detection, they can try to change the 802.11 channel of the APs in the area of the interference.

Some devices (Bluetooth or cordless phones) that cause noise actually change frequencies regularly, so it is impossible to change channels away from them. They consume the entire band at different points in time. It is critical to be able to identify the actual source of interference. Identify what the device is and where it is located in order to determine the best course of action to handle the interference. This may be removing or relocating the device. Another solution may be to shield the device from impacting the network.

Misconception 2: "RF sweeps in the site survey stage find all sources of interference."

One of the biggest challenges about interference is its intermittency. The interference may occur only at certain times of day (e.g. when someone is operating the device like a Bluetooth headset), or on certain days of the week. It is very easy for someone to introduce one of the many devices that operate in the unlicensed band into your environment at any time and thus it is a constantly moving target.

Misconception 3: "The WLAN network is working fine. There is no interference."

The 802.11 protocol is designed to be resilient to interference. When an 802.11 device senses interference, it will merely wait to transmit until the interference burst is finished. If the interference burst starts in the middle of an ongoing 802.11 transmission (and results in the packet not being received properly) then the lack of an acknowledgement packet will cause the transmitter to resend the packet. Packets get through, however increasing the PRC above 10% makes for an inefficient WLAN design.

The result of this waiting and retransmissions is that the throughput and capacity of the WLAN are significantly impacted.

Misconception 4: "A high density of APs solves interference issues."

The inexpensive nature of (especially thin) 802.11 APs makes it tempting to deploy them higher density than actually required, such as in every classroom. This type of deployment has the benefit of greatly increasing the capacity of the network.

Unfortunately, when deploying a dense network of APs, it is necessary to reduce the transmit signal power of each. If the power is not reduced enough, the APs generate interference with each other, known as co-channel interference. The reduction in the transmit power of the AP offsets the potential benefit of interference immunity. Therefore, the interference resistance of a network with a dense deployment of APs is not significantly better than that of a less dense deployment.

Distance

How far can you go?

The table below shows typical ranges that can be expected from an 802.11a/g WLAN design.

The reason for slower speeds is that material objects absorb the radiation. The amount of absorption varies with the material, but generally the more mass in the object, the more the absorption. Metal provides copious amounts of shielding due to how it interacts with electromagnetic fields. Furthermore, the angle that the signal passes through the wall affects the amount of interference.

Table 8 - 802.11a/g Speed and Range, Network Integrators of Canada Inc.

Speed*		Range*	
Throughput Speeds (maximum)	Effective Throughput Speeds* (typical)	Indoor	Outdoor
2.5	1	100 m	500 m
5.5	2.5	75 m	250 m
11	5.5	50 m	100 m
54	23	25 m	50 m

*Speed and Range defined here can be used as guidelines only and have been determined based on generally accepted industry information coupled with hands-on experience of WLAN implementations.

Or, if you are better working with graphical depictions, the below chart illustrates the same for an 802.11b WLAN with a maximum speed of 11Mbps.

Indoor

1.0Mbps @ 100 meters

2.5Mbps @ 75 meters

5.5Mbps @ 50 meters

23Mbps @ 25 meters

Outdoor

1.0Mbps @ 500 meters

2.5Mbps @ 250 meters

5.5Mbps @ 100 meters

23Mbps @ 50 meters

Indoor and Outdoor Speed and Range, Network Integrators of Canada Inc.

Electrical Requirements and PoE

The simplest answer here is Power over Ethernet (PoE). This should be utilized for all APs, otherwise the placement of APs must be within reach of a standard power outlet. As well, there are four options to power your AP. The options depend on whether or not the AP receives power from a power supply or if it receives inline power. The four connection options are:

- A switch with inline PoE;
- A patch panel with PoE;
- A power injector between the switch and the AP; and
- A local power supply (i.e. an electrical outlet near the AP).

If you use the APs 5-GHz radio, make sure your switch and patch panel provide enough power to the device. The 2.4-GHz radios are widely covered, but there might not be enough support for the 5-GHz radio.

Cabling Requirements

Points for consideration include:

- Each AP requires connectivity to a switch on the network. This often means more cabling runs must be pulled;
- Alternative solutions do exist, such as placing APs throughout the building or centralizing them using antenna extensions to distribute the AP. See Chapter 8 Case Study on Calgary Public's creative wiring methods; and

- Future-proof any cable that has to be installed. Use the higher rated cable to allow for future requirements. Using CAT6 instead of CAT5e, for example, ensures higher data rates reliably when required.

You must also consider the distance between the AP and the switch. The maximum range for 100BaseT Ethernet is 100 metres.

Physical Construction Elements

Building structure can be a significant source of interference. Most schools are constructed with concrete, brick and sheet rock. While materials, particularly concrete, will interfere with WLAN signals, sheetrock only blocks a small portion of a signal, making it WLAN-friendly. However, when deploying WLAN into older buildings, problems dramatically increase and may require the deployment of more APs than initially planned on paper. A detailed site survey of buildings will best answer this question. Older schools with wooden walls that were reinforced with a chicken wire-like material can cause significant interference and dead zones. Even though the material is not extremely thick, its shape and location throughout the walls and sometimes in the ceiling of a room effectively blocks, or at least disrupts, a WLAN's Wi-Fi signal.

Additionally, rebar-reinforced concrete can sometimes create a similar problem. This problem could be considered either a pro or a con. It can provide a way to secure the WLAN to concentrated areas and not have leakage of coverage outside of the building.

Both the type of material in an obstruction and the angle at which antennae point through obstructions affects signal degradation. Obstruction materials include plasterboard walls, cinder-block walls, concrete walls, glass with metal frames, metal doors in brick walls and steel-mesh reinforced walls. The greater the angle at which the antennae directs through an obstruction, the greater the signal loss will be.

A generic rule of thumb is that the signal is one-fourth as strong when twice as far away, barring any additional obstructions.

Security Considerations

The inherently open nature of wireless access, compared to the wired world, creates significant security concerns, chief among them, user authentication, rights enforcement and data encryption. Without the minimum recommended level of security as defined in Section 2.2 Wireless Security Standards, broadcast signals often travel into public areas that can be accessed by eavesdropping individuals who have not passed through any type of authentication process to validate their presence onto the WLAN.

The security solution must provide Network Access Control in different ways for different types of users who may require connecting at the same school, such as a teacher, student or visitor. Some users, such as staff or principals, may be entitled to total or broad access to all school and/or district resources. Other users, such as guests or students, may be entitled only to more limited access, like filtered Internet browsing.

The site survey should note where guests, contractors, or other non-staff users may be located, so that appropriate security solutions can be created for those areas.

Robust passwords form the foundation of security. They should be sufficiently strong to prevent easy guessing or hacking. Use both UPPERCASE and lowercase alphanumeric characters in addition to special characters. Use no less than a 10 character password. An example of a robust password is abc123XYZ!@#.

Impact of Device Standards, Ownership and Mobility

It is essential to understand the difference between non-standardized and standardized client devices, laptops that stay at school only versus ones that students take home, and one versus many device types to be supported by the district (e.g. Palm, laptop, BlackBerry, tablet A, tablet B, special device C, and so on). This section shows best practices surrounding security, optimal maintenance, support and management under the following scenarios:

School-owned: Standardized on Single Device Type (e.g. Laptop)

- This is certainly the easiest method to manage and support.
- Allows for easier management and support. All hardware is the same, each user group will have an image of the system that can be deployed for new users and correcting errors on old systems that are unstable.
- Support costs and mean time to repair will go down.
- Suspected that student acceptance is higher.
- Can have spare laptops ready for deployment or swapping (See Chapter 8 Case Study Evergreen Catholic School District).
- Can dictate access levels on the system itself and exhibit great control of the system environment to increase security and lower support costs.
- All laptops are the same regardless of user needs. Go with a balance of price and performance.

School-Owned: Multiple Device Types (e.g. Laptop1, Laptop2, PDA1)

- Can have spare laptops ready for deployment or swapping, however the more models/types to be supported dramatically strains budgets and support requirements (e.g. training).
- Can dictate access levels on the system itself and exhibit great control of the system environment to increase security and lower support costs.

- Allows for greater flexibility for user needs. Graphic users can have higher powered laptops whereby users that only do word processing (as an example) can be given lower cost laptops. There can be a tremendous cost savings here.
- Can still have spare laptops on hand for support and deployment.

School and Home Usage

At School Only

- Must have secure storage locations.
- Cart system. Trends indicate that although this is a common practice now, it will soon become common for students to take the laptops home.
- Accountability. What is the level of *ownership* and *attachment* students have to the laptops?
- Exposure is controlled and limited to school and district network only. Threats will be seriously minimized in this scenario.

Take Home and at School

- Recommended to have standard device type(s). This can be one single laptop make and model for every student across the district, or, multiple standard laptops and PDAs for association one-to-one initiatives.
- Laptops will be exposed to uncontrolled networks and possibly pick up threats and carry them onto the school's network.
- Increased support cost.
- Increased licensing cost to implement appropriate security, compliance, NAC, and so on.
- Some schools use VPN to enforce policy while on other networks. The laptop will not connect unless it can go through the school network and from there the content and security layers are applied to the traffic. This greatly lowers security risks but will increase technical support calls and support requirements.

Integration of Student-Owned Devices

Student-Owned Devices

- Lack of control. Users will likely have local administrative permissions.
- Best practise would be to dictate NAC control to force the user to keep their laptop up to security requirements outlined in the district's policy.
- Support them or not? Costs will go up if you are supporting these laptops. If not, then addressing strategy for a percentage of laptops failing during the school day is essential.
- Challenges with non-domain members. Authentication and integration with school systems may present a strong challenge. Join these to the school domain?
- Difficulty and decreased flexibility with one-to-one initiatives involving certain applications, any element going through district level networks, or even hosted application service provider software.



© Ken Hurst - Fotolia.com

- Security Policy
- Network Security
 - Network Based Firewalls and Traffic Topology
 - VPN and Proxy Servers
 - Intrusion Detection and Prevention
 - Virtual Local Area Networks (VLANs)
- Wireless Security
 - Avoiding Common Wireless Security Oversights
 - Network Access Control
 - Guest Access
- Mobile Host Security
 - Security Software and Operating System Updates
 - Personal Firewalls
 - Anti-Virus (A/V)
 - Anti-Spyware (A/S)
 - Encrypted File Systems(EFS)
- Content Security

Chapter 4 Security

This chapter illustrates a comprehensive top-down view of securing a WLAN, beginning with high level policies, network elements, security aspects specific to WLANs, addressing laptop and client issues and URL filtering. All elements in this chapter are positively correlated with a successful one-to-one initiative, as well as, a quality user experience while maintaining the high level of responsibility of a school.

In selecting WLAN hardware and management software infrastructure, it is best to choose APs that provide a comprehensive range of industry-proven security capabilities that integrate easily into any network design. Your WLAN hardware should provide standards-based authentication and encryption methods that satisfactorily address security concerns including authentication, NAC and data privacy. Additional layers of security such as VPN encryption should be strongly considered.

For very small school networks that function without a centralized RADIUS server for user authentication, some APs offer built-in RADIUS authentication. Your APs should integrate seamlessly with existing authentication systems, whether on existing school infrastructure or at the APs themselves.

4.1 Security Policy

Many districts are in the process of planning and deploying WLANs at school sites. It is vital to take steps to lock down wireless security by implementing written policies to guide users and administrators alike. Create a wireless LAN security policy now. It is the foundation of running a secure WLAN. If a policy is already in place, review and expand this policy to ensure it includes wireless specific and mobile user centric aspects.

Which areas should a wireless LAN security policy address? At the minimum, it should focus on seven key areas that establish the basis for deployment, use, and management of your wireless network. Details of each key area are as follows.

1. Define user base

Clearly identify who can use the WLAN and what level of access each particular *group* of users will have to both your intranet and the Internet. A good first consideration is to compare to the existing wired setup and policy to goals of the new WLAN deployment. You could choose to simply block a particular user group's wireless subnet from your intranet.

Regardless of how access is granted, it is essential to determine the scope of access. More important, clearly define this in your written policy and implementation.

2. Identify appropriate usage

After identifying the wireless network user community, identify the type of information that users can and cannot send over the wireless network. For example, prohibit sending personal information via the WLAN. In addition, prohibit ad hoc connections (i.e., peer-to-peer). Otherwise, savvy student users could extend your network to users who do not have authorization to use WLAN access.

3. Prepare for secure installation

Identify specifically which internal department and named individuals are responsible for deploying wireless within the network. Define minimum physical security standards for AP locations, and determine who will have physical access to the APs. Ideally, try to place your APs in controlled areas on the interior walls of the school. Adjust their coverage zone to the limits of your physical boundary, and not beyond, especially not into public areas like the road or parking lot.

4. Establish wireless security standards for the district

Define the minimum security measures enabled on all APs. Disable the service set identifier (SSID) broadcast feature, and change the default SSID to something that does not reveal a school or district's name. Enable one

of the strongest current available methods of wireless authentication and encryption as outlined in Section 2.2 Wireless Security Standards.

Check compatibility of WLAN NIC utilities. If disabling SSID broadcasts on APs, some systems may not be able to connect as desired.

5. Outline a contingency plan for loss of equipment

When the inevitable losses occur, your policy should stipulate immediately changing all the security settings within your wireless network (e.g., passwords and encryption keys). Best practices dictate to not store data on mobile devices, however should any data be on the devices, end-point security measures should be included. Treat any loss as a compromise of the system, and identify specific steps to take to mitigate further damage.

6. Plan appropriate training of both staff and users

Address training issues for the entire IT department as well as users to prepare everyone for the deployment, use, management, security, and incident response of the WLAN. Many districts often overlook this step during a new deployment. WLANs are completely different than conventional wired LANs. Outline a minimum training requirement, and develop a knowledge base for WLAN use from current successful implementations. Ensure that all staff are current on WLAN best practices.

7. Establish guidelines for management and monitoring

Once the wireless network has been deployed and locked down, there is no guarantee it will stay that way. The wireless section of your comprehensive security policy should define the frequency and scale of security assessments, which should take place on a regular basis to ensure continuity.

4.2 Network Security



© Kai Bankett - Fotolia.com

Network Based Firewalls and Traffic Topology

Firewalls are essential at both the school site and district head office. If school sites access the Internet directly and do not follow a hub and spoke traffic topology, it is absolutely essential to employ firewalls. Most firewalls today have bundled security features such as VPN capability. Firewall should be deployed to protect critical network servers not only from external Internet traffic, but even more importantly to protect against internal unauthorized access attempts by users like curious students. Installing firewalls at both the school and district level will allow for any outbreaks or threats to the entire network to be isolated quickly.

Firewalls should be installed to protect entry points and network perimeters. Ideally they should also have IDP/IDS (Intrusion Detection and Prevention) capability.

There are essentially two different methods of schools accessing the Internet. Schools' WLANs access the Internet directly whether via an ISP (Internet Service Provider like Shaw or Telus) or via SuperNet. As well, schools access the Internet via the district head office, referred to as a hub and spoke topology. The differences are how much firewall and security capability is at each school location, and aggregate bandwidth requirements for centralized traffic and control from the district level. Either method can be secure and functional. A district's current investments should be analyzed here to determine the best way to leverage investments already made.

If using the distributed method of each school accessing the Internet directly and not routing traffic through the district office, it is strongly recommended to use centrally manageable security appliances. Push central policy settings to managed appliances such as Fortinet or Check Point at school sites over the district's Internet connection. Several business-class network appliance providers offer products that combine VPN, WLAN (including WPA2), firewalling, URL filtering, VLANs and NAC support (see Table 9). Additional software is often required to augment and provide greater functionality, such as reporting on individual users URL attempts or more granular spam and virus management.

Table 9 - Firewall Vendors and Products

Vendor	Product	Price Range (\$) (hardware only)		Gateway Anti-Virus	Integrated WLAN?	Other
		Low	High			
Check Point	Safe @ Office500W	250	1,000	Yes	802.11a/b/g, Super G, XR, WMM	Can support 4 VLAN security zones. 5, 25 or unlimited user versions available
Juniper Networks (acquired Netscreen Technologies)	5GT	950	1,500	Yes	802.11a/b/g	Firewalls, IDS, IDP and other services are offered on separate stand-alone devices.
Fortinet	60wi-fi	750	1,250	Yes	802.11a/b/g	Launched by founder of Netscreen Technologies.
Aruba	AP-41 AP-65	250	500	No, (integrates with Fortinet)	802.11a/b/g	A leading smaller vendor with solid solutions for K-12
Cisco	870 1800	750	1,500	No	802.11a/b/g and dual mode WMM	Largest company in terms of revenues, number of deployments and history. The overall market leader.

These products range in price from \$250 to \$1,500, which makes them affordable to implement at individual school sites. IT budget managers must recognize that these devices will simplify remote support and will automatically reduce vulnerabilities because they accept and enforce central security policies. Should students access the Internet at school, or connect to the school's network from home, the security features, including URL filtering, are driven by these devices.

Under the other school of thought, implementing a centralized hub-and-spoke model allows for superior equipment to be implemented at district head office. The vendor licensing agreements will reflect pricing levels of the number of schools and throughput connecting to the Internet via your firewall. Speed will be another element for consolidation, and the district head office will need to have one or multiple managed SuperNet connections from Axia in order to handle the consolidated traffic from all schools.

Virtual Private Networks (VPN) and Proxy Servers

Configuring VPNs to communicate between schools and head office is critical for ensuring the traffic integrity. VPN client software can then be deployed on student systems allowing remote, after-hours access to resources they need to complete homework. This is an excellent way to enforce students' Internet access while not on school premises to flow through school or district resources, and thus be monitored and protected in line with the security policy. Students would be able to use the Internet and resources exactly as if they were physically at school.

There are proxy server solutions which could address basic Internet traffic management of off-site students, however, these are not as capable of monitoring and managing as a VPN solution. One example would be simple access to files or centralized/hosted resources.

Intrusion Detection and Prevention (IDS/IDP)

Deploying network wide IDS/IDP (including WLAN IDS/IDP) is the most secure. This protects the network from attack attempts and can alert you of unauthorized activity. Logs and analysis of how users attempt to gain access to the network can be compiled. This data can be used in future network upgrades and designs.

It is recommended that at minimum a WLAN Intrusion Detection System (IDS) or an integrated Intrusion detection and prevention solution. The latter not only identifies intrusions, but also addresses them automatically.

Virtual Local Area Networks (VLANs)

Isolating different user types (grouped by their functional requirements) into VLAN network segments and firewalling between VLANs will greatly increase security. Furthermore, isolated users may only access exactly the resources they require, which helps with overall IT resource management and decreased support requirements. Different user types or groups are isolated from one another for further protection of peer-to-peer breaches.

As WLANs scale out more users, VLANs also isolate network traffic to help control and reduce bottlenecks associated with large, flat networks. As application adoption and usage increases, this management technique will provide maximum control of bandwidth, and ultimately cost.

4.3 Wireless Security

Because of the nature of wireless signals, it is impossible to stop anyone within the signal range from attempting to access the data or the entire WLAN. This is the nature of wireless technology. Fortunately, there are security methods available today to address these security concerns. It is typically a matter of policy, will and budget.

In reality, not all WLANs are configured and deployed in an ideal manner with secure access and authentication. As such, one of the main issues with that WLANs is unauthorized access to network resources and unnecessary traffic. The following will help identify common pitfalls and associated challenges in wireless security.

Avoiding Common Wireless Security Oversights

Here are the most common security oversights and how you can avoid them.

1. Breached Firewalls

Most schools have firewalls around the network, wireless or not, and rightly so. However, if the configuration does not isolate the wireless network from firewalled resources, then the level of control diminishes. Make sure it does, otherwise there is no barrier (the entire point of the the firewall) should an unauthorized user acquire wireless access.

2. Spurned Media Access Control (MAC)

MAC is often ignored because it is not spoof-proof. It should be considered another brick in a district's overall security strategy. It is essentially another address filter, and it clogs up the works for the potential hacker. It limits network access to registered devices that you identify on address-based access control database.

If you have MAC in place, the intruder must bump into it before even realizing it is there, and then attempt to get past it. So now the intruder is known. A MAC list creates three classes of visitors. First, friendly entities are on the MAC's list; second, unknown entities that are not on the list and who knock by mistake; and third, entities who are not on the list but are known because they have tried to get in before, uninvited, and are now instantly identifiable if they approach again.

MAC address filtering directs the AP or a RADIUS server configured with the MAC addresses of the permitted wireless clients to be granted access. Unfortunately, this method by itself is not secure because frames could be sniffed to discover a valid MAC address, which the hacker could then spoof.

WLANs require the same security policies as wired networks, but it takes more steps to get there. The same issues that are of concern in the wired world should still be of concern with WLANs and devices. Keep encryption strong, keep certificates in place and manage security in an ongoing fashion. Wireless security is not a matter of different security; it is a matter of more security.

3. Use the highest level of authorization and encryption

Refer to Section 2.2. This is often the weakest link in a wireless security infrastructure, but it can be addressed through the use of continually updated best practices.

4. Allowing unauthorized (rogue) APs

Have a procedure in place for noting the presence of neighbouring APs and a policy of how to deal with newly discovered rogue APs on the wireless network.

5. Permitting ad-hoc laptop communication

This is difficult to enforce in any environment. The ad-hoc mode lets Wi-Fi clients link directly to another nearby laptop, say from one student to another. As part of the 802.11 standard, ad hoc mode permits a

laptop's NIC to operate in an independent basic service set configuration. This means that it can go peer-to-peer with another laptop via RF. Note that this permits access to the entire hard drive of the laptop, which will prove to be a recipe for disaster amidst eager young minds.

Be aware of potential new applications being pitched for deployment on the WLAN if they require any sort of peer-to-peer element. These applications should be rejected from the highest level of the security policy.

6. Not Protecting Legacy WLAN Investments

The best answer for legacy WLAN equipment is to replace it. If that is not feasible, then it should be isolated on a separate network with firewall separation or virtual LAN (VLAN) that blocks access to other school or district resources. Only the expected data should be allowed to flow, and only to a pre-authorized address and/or gateway.

If the devices do not support reasonably strong legacy wireless security, but can support a VPN, then the VPN should be activated, and security settings should be made as strong as possible. VPNs run independently of the WLAN and are immune to weaknesses in the wireless security protocols. If users need to roam, this option will prove difficult with the Internet Protocol security, because it does not tolerate interruptions and IP address changes. Secure Sockets Layer (SSL) VPNs and proprietary mobile VPNs can support roaming where required.

Data traffic and applications allowed to run over the legacy wireless system should be limited. Bar access to unnecessary network resources and applications.

Migrate to Wi-Fi Protected Access 2 (WPA2) compatible WLAN network interface cards, drivers, supplicants, and APs for all new purchases.

Network Access Control (NAC)

NAC is a security layer implemented at either or both hardware and software that performs robust and higher level checks of the client's security state prior to authorizing access to the wireless LAN and/or specific resources on the network.

Some of the checks include installed patches, anti-virus protection status and what applications are or are not running on the client. NAC automates compliance enforcement. Examine three choices for access control. First, implementing access control through routing and switching hardware, purchasing appliances or exclusively as a software solution. These three options can be mixed and matched and it should be noted that:

- Using routing and switching hardware gives the most granular control and flexibility.
 - Capability of tying policies to access control dynamically. Instead of telling a switch to admit or deny a device based on some fixed attribute such as its MAC address, it can make decisions based on policies that vary, and on compliance with those policies, which can also vary. The benefits of this approach are that it offers the highest performance and it is the most scalable solution.
- Using a hardware appliance is less expensive
 - An alternative that avoids replacing relatively new switches is to adopt access control appliances to do the work "in a box". This completely avoids touching the existing network infrastructure — access control is effectively implemented as hardware overlay — and is likely to be considerably cheaper. The disadvantage of this approach is that it is less granular, less scalable and its performance is likely to be lower.
- Software solution is fastest and least expensive, but offers no control at layer 2.
 - There are plenty of vendors such as McAfee, Check Point and Endforce that supply products to achieve this. The downside is that where a network appliance has lockdown capabilities and can shut off access

to a user at the network layer 2 or 3 level (effectively carrying out a function which has been offloaded from the switch), software does not provide this level of control. The most likely scenario is that the software is used to prevent hosts being assigned an IP address, or only an address from a particular, restricted range.

It is important to reiterate that these three architectures can be mixed and matched — it is perfectly feasible to install new switches at the district head office, an appliance at one school and software solutions at other schools. Or you could install appliances or software as an interim measure, and to replace them with new network hardware when it is time to replace it.

Compliance is critical, especially for laptops that will be going home with students. If the A/V is not up-to-date, the firewall has been disabled or the latest security patches are not installed, the device can be denied access, quarantined and directed to a self-help remedy portal that directs them on how to correct their system to gain access. These online portals are typically supplied by the vendor, and will assist in lowering the support requirements in this area as well.

Make sure that the solution is (Cisco) NAC or (Microsoft) NAP compatible. Cisco and Microsoft have formally announced interoperability between the Cisco Network Admission Control (NAC) and Microsoft Network Access Protection (NAP) solutions.

Guest Access

Guest WLAN access is convenient for visitors who increasingly require Internet access to do their jobs. This could include temporary administrative staff or supply teachers, consultants or even your District staff who may carry laptops and visit many different school locations. District WLAN access must be segregated to minimize security exposures and conflicts of interest.

Use VLANs as the most-cost-effective way to segregate guests and divert them to the Internet. VLANs are easy to set up within your school networks and are supported by the major LAN equipment providers, such as the intelligent routers and firewalls in place at school sites now.

Many business-grade WLAN equipment vendors have guest access management systems that provide a sign-in screen, guest password and a method to expire guest access. The best systems provide a browser landing page and will register users "on the fly" or with a password supplied for guests. Use the guest access system supplied with the WLAN vendor's equipment and/or LAN NAC system if it exists.

Ensure that guests to sign a user compliance agreement before activating guest access. Guest users should, at a minimum, be required to click "yes" on a browser screen that indicates they agree to terms of privacy and conduct, and assigns to them any liability for their actions. This feature should not be bypassed for the convenience of guests.

Require guests to obtain a temporary access password. Network security is better served by requiring guests to sign in with a live person, such as the school secretary or even vice principal, who can then issue a password that the guests can enter into the sign-up screen.

Track guest access by wireless NIC MAC address. A wireless guest should be required to sign up for each wireless device that needs access. Typically, this will be one device, and usually a laptop. The MAC address can be captured during guest's initial entry and checking in at the school office, and will assure that your guests cannot share the password. Only their own device can be used, and the responsibility for following your access rules will belong to the person who accepted the guest access agreement.

Expire guest access credentials on a daily basis, or more frequently as needed. Guest access should be treated like a sign-in sign-out sheet, and should be expired as soon as it is no longer needed.

4.4 Mobile Host Security

Mobile host security means securing the laptops and other devices that come on and off of a school's WLAN. This is accomplished with a broad mix of technology and best practices of users complying with a sound wireless security policy.

Introducing mobile computers into your network on a large scale will impact security. They move from network to network and their exposure to vulnerabilities while outside of the school WLAN are unknown. They can be physically compromised and data can be stolen.

Security Software and Operating System Updates

Desktop and laptop patch management should be deployed to ensure the latest product patches are pushed to all clients. This will help to increase security, reduce compatibility challenges, keep interfaces consistent and decrease support costs over time.

Have a comprehensive desktop management strategy that includes all mobile devices and laptops. A comprehensive, centralized dashboard to monitor, maintain, manage and report on all desktop management aspects. Do not settle for just patch management software. The feature and functionality set of the chosen management system should be comprehensive and in one simple Graphical User Interface (GUI).

Personal Firewalls

Personal firewall software should be deployed on each and every laptop. Ideally, these software firewalls will function within a centrally controlled system that can enforce usage with and is compatible with your hardware firewalls.

All laptops with a wireless NIC must have a personal firewall installed that supports connection-specific policies. As laptops are often outside the protection of the school or district firewall, every laptop should have a personal firewall installed. This will be critical for students taking their laptops home and then returning, with potential infections, to the school WLAN. The firewall built into Vista may provide sufficient baseline security for student laptop use, although software client licenses compatible with your firewall solution at either the school site or district head office is better. What is built into Windows XP is not sufficient. The personal firewall should be configured to block split tunnelling and any ad hoc WLAN connections.

Anti-Virus (A/V)

A/V protects and minimizes threats, and is essential for all laptops because new viruses proliferate daily and spread quickly. A/V should be centrally controlled so the definitions can be monitored. If not, definitions may not be updated and laptops would eventually get a virus. MacAfee, Symantec, Trend Micro, Computer Associates and many other vendors have central control and monitoring.

Despite offerings for stand alone, typically consumer versions, do not implement these as they do not have central management and require maintenance and updates. Some small districts may have this in place on guest or even existing legacy laptops accessing their WLANs. This practice should stop immediately.

Anti-Spyware (A/S)

A/S protects against threats through the Internet browser. Protecting against this will dramatically reduce the level one technical support requirements and support time and costs. Fewer users asking to have their system cleaned means more time for more important projects or additional training.

Pop-ups can be frustrating and will impact a user's experience. A/S can protect against these as well.

Encrypted File Systems (EFS)

Security certificates and critical data will be accessible to a savvy user who happens to come across a lost or stolen laptop, and includes all access settings to the WLAN and other resources including applications, VPN and more. Using EFS, systems will make it challenging, if not impossible, even for a highly skilled user to crack and gain access without the user's network password. In this scenario, password policy and enforcement is critical.

The key to address here is that if a laptop is lost, no one could access the data on it. Imagine if a principal's laptop were stolen while travelling and all of the private data therein were exposed to a thief.

4.5 Content Security

The scope of Content Security typically covers the following:

1. Website Surfing Content Control (i.e. filtering unacceptable URLs)
2. Controlling use of Instant Messaging Applications
3. Controlling Access to file sharing Peer-to-Peer (P2P) Networks

Traffic between computers, APs, controllers, switches, firewalls and other network appliances can be controlled significantly by implementing Content Security policies and technology.

Features and specific functionality vary between vendors and types of technology solutions. Solutions can include blocking categories or websites (such as adult or gambling), ad-hoc white and black listing websites, keyword analysis and resolution (even if contained within an e-mail, instant message or websites) and more.

Solutions exist for both centralized or distributed control. Most firewalls released in the last year have integrated solutions that may be more cost effective than an entirely separate system. Centralized control is generally recommended as it eases administration burden and can give management high level reports of the entire organization's activity.

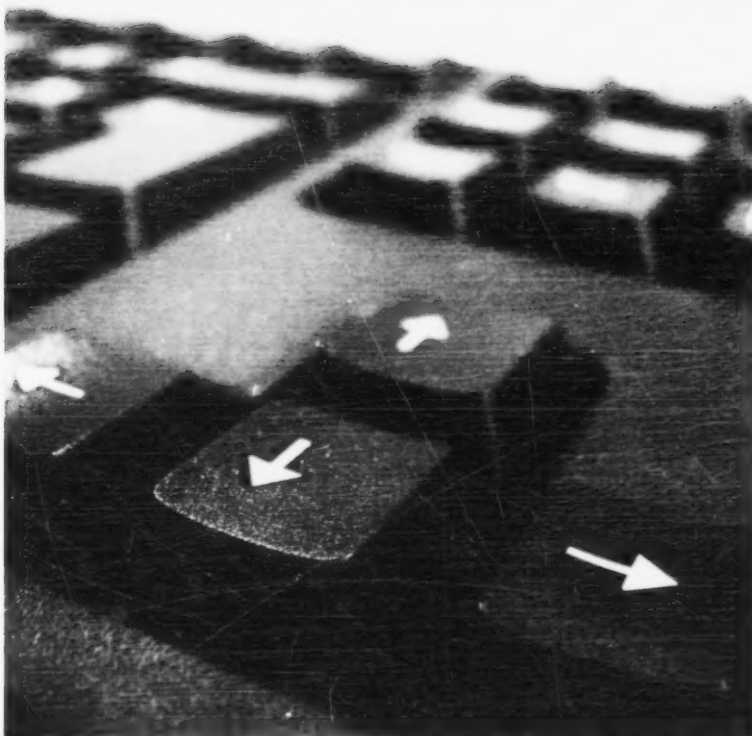
Used effectively in conjunction with a hub and spoke traffic topology, districts can control users' content while they are on the school WLAN or using their laptops while on another network.

Some sample vendors in this space include:

- www.symantec.com
- www.8e6.com
- www.fortinet.com
- www.checkpoint.com
- www.barracudanetworks.com
- www.surfcontrol.com

These types of solutions are only as good as they are configured and installed in line with the vendor-specific feature set. Often, there is a channel partner, consultant or even you existing VAR (Value Added Reseller) who may be a better first line of communication and sales for these Content Security solutions.

Chapter 5 Making the Best Decision for your School(s)



© Benis Arapovic - Fotolia.com



© Eric Simard - Fotolia.com

Chapter 5 Making the Best Decision for Your Schools

The best way to look at this is in a holistic manner. This is not, and should not be, viewed as a simple hardware selection. Moving into the wireless and mobile user space involves every aspect of technology across the district, and likely a few new elements.

By this point, it is easy to be focused on the technological aspects of these solutions, perhaps frustrated with not having an extensive understanding of the complex inter-relation of all technology pieces required to implement one-to-one initiatives. It is strongly recommended that you use your core expertise in understanding the fundamentals of delivering education to grow students' experience and knowledge as the base of your decision making.

Whatever the mix of technologies used to deliver a one-to-one initiative, it should not disrupt the learning process. In the early stages of the province rolling out one-to-one initiatives, a measured pace is encouraged to be able to monitor the impact of WLANs and all associated new technology. Real feedback from teachers, IT staff and students will prove to be the best guidelines on making improvements.

Size does not matter. Whether a one-to-one initiative is set to involve 25 students or 250, the number of students is not correlated to the project's difficulty, budget requirements or unique educational and technology challenges.

It is also imperative to complete a one-to-one project in its entirety prior to increasing its scope. Any scope changes should be scrutinized through a decision making process which takes into account all non-technical factors and issues addressed in this guide.

One-to-one Initiatives Today and Tomorrow

Ultimately, what will weigh the heaviest on decisions surrounding WLANs is the application of their goals for today and tomorrow. These are the definitions of the one-to-one initiatives themselves. There is a vast variety of one-to-one projects underway. Some will be simple to implement and manage and may only utilize basic web browsing, while others are very complex requiring more time, attention, training, budget and technological commitment to see them succeed.

One-to-one initiatives are not too different than implementing any other new kind of education model, whether that is visual learning, special education, physical education or the advent of a calculator or typewriter. The following chart highlights 25 correlated factors affecting the success of an initiative.

Key Inter-Related Elements of Decision Criteria on IT Strategy when Implementing WLANs

Current one-to-one	Non-Technical Factors	Traffic Topology	Desktop Management	Timeline
Technology Trends	Community Concerns	Growth and Adoption Rates	District and School IT Staff and User Education	Number of School Sites
Number of Laptops	Security Tolerance	IT Staff and In-House Skills	Standardized vs. Non-Standardized Clients	Budget
Number of Student WLAN Users	Existing Network Hardware	Out-Sourced IT Service Partner	Scalability	Mobility Requirements
Application Characteristics	Future one-to-one	WLAN Vendor	Life Cycle	Ongoing Support Requirements

For example, having a known budget of \$500,000 and arbitrarily selecting five school sites with 50 students and laptops at each school is fine. However, once other variables are factored in, it may be discovered that this number of students and schools requires an additional \$200,000 of infrastructure upgrades. Or, maybe the mobility requirements and community concerns are not in line with the security tolerance mandated by the implemented budget level.

This is not being presented to say that it is impossible to achieve fantastic results in a secure environment and allow a maximum number of students to enjoy the program. It is being noted to help decision making happen at the encompassing level. This is what is required to avoid surprises later, once commitments have been made.



© Jake Hellbach - Fotolia.com

- Implementation Checklist
- Communication
- Piloting and Roll-Out
- Documentation
- Trouble Shooting Tips
- WLAN Performance Testing and Tuning

Chapter 6 Implementation

The implementation phase should not be daunting or filled with surprises. As addressed in Chapter 3, you need to take the entire project plan and determine the unique items to add to the following checklist template.

Checklist

Below is a sample, high level checklist to assist with WLAN implementation. It includes items that are required before WLAN implementation, such as infrastructure upgrades. WLAN vendors will have specific project plans and checklists that include proprietary or unique steps in setting up their hardware and software. Read through this documentation, and then assign this to the central and primary project manager responsible for the overall WLAN implementation.

Note that the pre-WLAN projects could likely take more resources and time than the actual WLAN portion of the setup. Each below listed item could be expanded to include subsequent projects and new school sites.

Table 11 - Implementation Checklist, Network Integrators of Canada Inc.

Item	Completed
Pre-WLAN Implementation Items	
Existing hardware upgrade project 1	
Existing software upgrade project 1	
Existing network architecture upgrade project 1	
Internet connectivity upgrade project 1	
Architecture project upgrade 1 (NICs, VLAN supporting firewalls, etc.)	
One-to-one Applications to be run on the WLAN installation	
Power requirements for each AP (coordinate district electrician) or install PoE hardware	
Run patch cables between your wired network and each AP	
Record the MAC address of all hardware	
WLAN Implementation and Security	
Configure and install WLAN controller	
Install a pilot set of APs at one location	
Configure clients (e.g. Standard setup for a one-to-one laptop)	
Test and fine tune client:AP ratio	
Adjust AP and antennae placement	
Record physical location of all hardware (by MAC addresses), use floor plans	
Roll-out all APs at all locations	
Configure remaining clients	
Test and Fine tune all	
Configure and implement security settings for VPN, VLAN, NAC and/or other hardware and software (advised to perform on pilot area, test, then roll-out)	
Vendor product training on Controller management software. Reset all passwords to high level of entropy, get familiar with interface, features, capabilities and reports	

Communication

All technical implementation team members should have a master project folder that includes the following items:

- Alberta Education WLAN Best Practices Guide;
- District Security Policy;
- Vendor contact;
- Project team contact;
- IT management contact;
- Other contact info (school or district maintenance, etc.);
- Project plan;
- Floor plan of all sites;
- Roles, goals and responsibility list;
- Schedule;
- Deadlines;
- All associated vendor documentation (hardware, software or other); and
- Blank inventory sheets. Do not underestimate pen and paper here.

Time and frustration are the two biggest items saved by having clear and consistent communication amongst the technical implementation team right up to the senior management ultimately responsible for the project.

Piloting and Roll-Out

Regardless of the size of the school district and the depth of its IT staff, the implementation team should follow the pilot methodology. This will save time in the overall project, and offer an opportunity for junior IT staff to gain valuable experience and training alongside senior members of the technical implementation team. The pilot phase should not be rushed as it provides a valuable knowledge transfer to the junior IT staff members, which is essential to build in-house skill-set.

Technical hurdles must be overcome during the pilot phase to minimize any potential negative impact on one-to-one initiatives as full roll-outs occur.

Documentation

Inventory of Wireless Devices

All serial numbers, makes, models, MAC addresses and locations should be documented. This information will be required when contacting vendor support during setup or thereafter.

Read all Vendor Information

Valuable tips and information will be recorded in the vendor documentation. Generally, the vendor wants the setup experience to be positive, and will pack as much helpful data into the documents as possible.

Record all Support and Contact Information

Record all technical support numbers and support contract details. This information should be delivered to any technician on the implementation team who will be performing setup or trouble-shooting. Having this information will greatly speed up implementation.

Include internal IT project team members and senior management for clear and immediate communication as required during a swift setup.

Trouble Shooting Tips

Challenges can arise when implementing a WLAN. The following checklist should help your district's technical team resolve many of these challenges.

When a wireless network fails, there are eight areas to look to first:

1. Swap the troubled AP for hardware troubleshooting;
2. Test signal strength;
3. Try changing channels;
4. Verify the SSID;
5. Verify client encryption settings;
6. Verify AP connectivity ;
7. Verify wireless controller connectivity; and
8. Verify connectivity to DHCP server.

WLAN Performance Testing and Tuning

Testing Methods and Devices

Wireless LAN Assurance Tools are available from various vendors as either hardware or software, including free versions to be placed on a laptop. This will help with the initial site survey and ongoing management for items like interference, signal analysis and rogue AP detection. Here are a few vendors listed to begin your research in this area:

Fluke Networks:	www.flukenetworks.com/wireless
Air Magnet:	www.airmagnet.com/products/laptop.htm
WildPackets:	www.wildpackets.com/products/omni/overview/omnipeek_analyzers
AirMagnet:	www.airmagnet.com
Network Stumbler	www.netstumbler.com This is free software to be loaded onto a Wi-Fi enabled PC
Tektronix	http://www.tek.com/products/communications/products/wireless/index.html
Cisco	Aironet Desktop Utility, which includes a site survey tool component. This tool allows you to view the strength of your APs signal, the quality of the signal, packet retries, and a host of other data.
Cognio:	www.cognio.com

There are also devices called Spectrum Analyzers that identify arbitrary wireless signals. They are typically too expensive (\$10,000+) to purchase for anyone other than large enterprises or service providers and require specific training for proper use.

Fine Tuning

Measuring Signal Strength

In conducting the site survey, make sure that the proper equipment and tools are available and present. That equipment can be relatively simple, including the APs, antennae and wireless stations that will actually be used in the deployment. Place the AP in locations where it is likely to achieve appropriate coverage and then measure the result. With the AP in a given spot, move the wireless station to various locations and measure the signal strength, noise level, packet retry count, signal to noise ration and other data rates produced. Take several measurements from each location to assure consistent results.



© Galina Barskaya - Fotolia.com

- Calgary Board of Education
- Calgary Catholic School District
- Evergreen Catholic School District
 - Introduction
 - Cost Saving Techniques
 - Vendor Selection
 - Implementation
 - Security
 - Maintenance and Support
 - Lifecycle
 - Conclusion

7.1 Introduction

Several school districts throughout Alberta have already begun and completed wireless network installations at some or most of their schools and are well on their way to implementing one-to-one laptop initiatives. We were requested by Alberta Education to contact these districts and learn about their experiences in an effort to share information to help all districts implement and manage their wireless networks.

The school districts interviewed included University of Calgary, University of Alberta, Red Deer College, Calgary Public, Calgary Catholic and Evergreen Catholic. All were very generous and open about their experiences and we hope that sharing this information will help your district understand and utilize best practices for implementing and managing WLANs, as well as save time and money.

In the following three case studies, we look at each district's particular concerns, challenges and decisions regarding cost, vendor selection, implementation, security, maintenance and support and their WLANs.

7.2 Calgary Board of Education (CBE)

Introduction

The Calgary Board of Education (CBE) is the largest district in Alberta. It has allocated extensive resources to their IT infrastructure and have aggressively installed wireless networks into more than half of its schools. It has created a unique implementation through careful planning and extensive research. Its redundant IT infrastructure is managed entirely in-house and it has more than 150 IT staff members.

Cost Saving Techniques

CBE's wireless network pilot projects showed that in order to gain 100% wireless coverage in all schools, it would have to double the number of access points in order to cover the final 20%. The resulting cost would have been far too great, so it decided to re-design the way it deployed wireless access points. Instead of installing access points in classrooms, closets and hallways, it installed the access points centrally in a wiring closet and extended the antennae by running a single cable per access point through the school. This resulted in a dramatic cost savings in both cabling and number of access points required to cover 100% of the school area. By centralizing network services, CBE gains economies of scale on licensing and management. Services such as storage, authentication, content filtering and e-mail are all managed centrally.

Vendor Selection

CBE sticks with brand name hardware vendors only and selected Aruba for its wireless network infrastructure, specifically access points and controllers. It is in the process of upgrading the switching environment to Nortel products and is using Check Point to firewall the network at district head office level.

Implementation

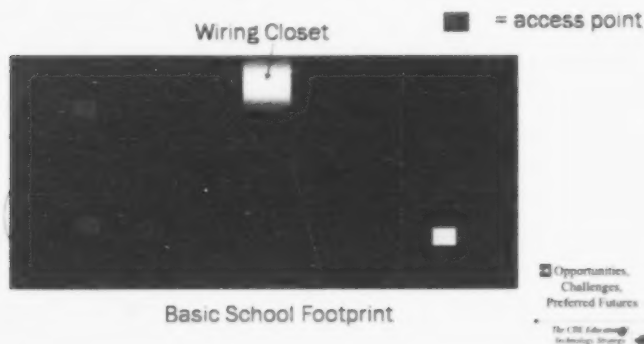
CBE has come up with a unique installation design for its access points. The traditional installation of site access points (fixed access point solution) requires a network cable to be run to the location of the access point. This often will require hiring contractors to install new network jacks throughout the building.

Calgary Board of Education Summary

- *100,000 Students*
- *13,000 Staff*
- *235 Schools*
- *125 Wireless Networks*
- *Unique, Cost Saving Access Point Deployment Method*
- *"Brand Name" Hardware Only*
- *Over 150 IT staff*
- *All Work Done In-House. No Outsourcing*

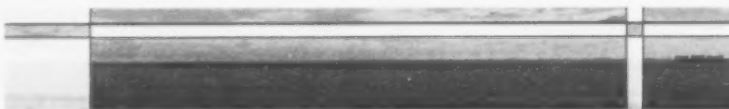


"Fixed-Access Point Solution"

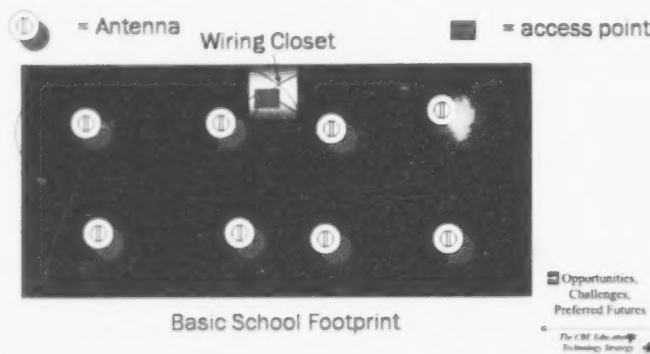


Source: Background on the Wireless Distributed Antenna Deployment (WDAD) Project (PowerPoint)
http://projects.cbe.ab.ca/sss/ilcommunity/learningspaces/wireless_files/WirelessProjectBackground.ppt

The installation that CBE came up with does not require multiple network drops to be installed. Instead, it installed antenna extension cables throughout the school running them all back to a central wiring closet. It connected these cables to the access points installed in the closet and anywhere it required coverage, a simple antenna (\$30-\$40 cost) was attached to the antenna cable.



"Antenna Solution"



Source: Background on the Wireless Distributed Antenna Deployment (WDAD) Project (PowerPoint)
http://projects.cbe.ab.ca/sss/ilcommunity/learningspaces/wireless_files/WirelessProjectBackground.ppt

This allowed CBE to dramatically reduce the cost of installation, as well as benefit from the added physical security and lower replacement costs due to the centralized location of the access points. It now has about 190 schools wired for wireless network installation and about 125 active wireless networks.

During the pilot process the CBE also found that getting 100% of coverage in most schools required twice as many access points than were required for 80% coverage. The antenna solution allowed it to gain the 100%

coverage without the need for extra access points. Each cable can run four non-overlapping channels allowing four antennae to be installed per cable.

Bandwidth is shared at each access point and the CBE found that if it did not keep the user-to-access-point ratio low, performance drops would occur under certain circumstances. An example of this is at one high school the login script would download a relatively large image file of and when entire classroom logged in at the same time, the wireless network performance would degrade.

Power over Ethernet (PoE) is used to power the Access points in the closet eliminating the need for more electrical outlet installations. Services such as storage, email and content filtering are centralized in CBE's main network operations center (NOC). A redundant NOC is setup providing failover services for their most critical systems. Full application redundancy is planned and some implementation is under way. CBE utilizes Microsoft technology almost exclusively for its entire IT infrastructure.

The main NOC uses multiple 60Mbps SuperNet connections to handle school traffic. There is no load balancing across the handful of connections, and requires manual load balancing by assigning each school to one of the connections.

Security

The access point installation solution that CBE uses does leave some signal transmitting outside the building. This is limited, but may be a concern to some boards. Each school site uses a different set of encryption keys and SSIDs. Access to the network is limited by RADIUS authentication. In the event that an intruder gained access to the encryption keys, the IT staff would be alerted to the unauthorized MAC address. A secure switching architecture is installed to also add control of the MACs that access the network. Rogue access points can be detected and located if plugged into the network.

Non-CBE devices are isolated on their own wireless network and their traffic flows straight out to the Internet from the school's connection without going through the district head office hub-and-spoke configuration. All internal network access is restricted to CBE-owned devices only. WPA or WPA2 is implemented for security. SSID broadcasts are disabled. Content filtering and anti-virus solutions are deployed to protect end users.

Maintenance and Support

CBE employs over 80 IT staff to support the schools and about another 80 staff to support the head office and data centers. The NOC group consists of four staff. Together it supports more than 40,000 devices. It does not outsource maintenance or support and prefer to use the existing staff to perform all the work.

Senior high schools have a resident technician while multiple junior high schools and elementary schools are supported a single technician. Some staff at the schools are junior and do not work with servers. Only senior administrators are allowed to maintain the servers and sometimes it are required to support multiple schools, both remotely and onsite. The first line of support is the teachers themselves. Students can speak to them and teachers can call the help desk to initiate a support request.

Lifecycle

The life cycle of a server is three years, five years for desktops and three to four years for laptops. Sometimes it stretches the laptop use to five years. The life expectancy for the access points is three to five years, for the antennae it is five to seven years and for the antenna cable it is 15 to 25 years.

Conclusion

CBE has put a tremendous amount of thought and planning into its wireless network solution. Its IT staff is highly organized and committed, and this is reflected in the design and implementation of the entire enterprise network. Its solution is innovative and functional and can be a cost effective design for school districts of all sizes implementing wireless networks.

7.3 Calgary Catholic School District (CCSD)

Introduction

The Calgary Catholic School District consists of 98 schools with plans to increase to 102 schools next year. It currently employ an IT staff of approximately 35 and manage 10,000 PCs and 150 servers. It has already installed wireless networks in 11 schools and has been using mobile cart solutions since 1999.

Executive Summary

- *44,000 Students*
- *2,500 Teachers*
- *98 Schools*
- *11 Wireless Networks*
- *Aruba Solution. Wireless Switches and Thin Access Points*
- *IBM Desktops and Servers*
- *Toshiba Laptops*
- *Outsources Time Intensive Tasks to Optimize Maintenance And Support Budget*
- *Tight Control of Wireless Signal Transmission and Access Times*

Cost Saving Techniques

About 75% of its IT budget is set aside to cover staffing alone, leaving the balance for other expenses such as hardware, software licensing, outsourced support and training. The Board is careful with every decision it make regarding IT.

To help relieve the strain on Calgary Catholic's budget, it purchases all hardware with a minimum three-year warranty. The onsite service call required to perform this work is included in the original purchase price. Contracts for out-sourced support are mostly flat and any and all work that is billable is subject to a maximum rate and is open for audit prior to payment.

All testing performed by students on computer systems happens in a temporary lab on desktop systems. The hardware setup and tear down are all completed by a vendor for a fixed rate. This periodic task is time consuming and would eat a lot of in house IT staff time and is an example of something perfectly suited for outsourced IT help.

Another example of time intensive work that takes away in-house support staff time is the ongoing support of firewalls, anti-virus software and spam filtering systems. Calgary Catholic is also exploring out-sourcing all of these services to a third party.

Vendor Selection

Calgary Catholic uses IBM exclusively as its server and desktop hardware platform. All laptops and printers are from Toshiba. It purchase from a VAR that is well established and has multiple offices, making it well suited for supplying and supporting the geographically dispersed schools.

The district has also creates what it calls "a three-way partnership" with the reseller and the manufacturer whereby they both provide support, guidance and planning for the board's entire IT infrastructure. This provides CCSD with access to industry experts through an existing strong relationship when it is looking to embark on complicated IT projects and ensures that the reseller has direct access to support from the manufacturer of the hardware. For wireless networks, centralized management was a key criterion for selecting Aruba as its vendor.

Implementation

The roll-out of its wireless networks consists of installing 14 access points for up to 60 users. All signals are tuned so that the network is not broadcasting outside any school walls. This is achieved by walking around the school with laptops and where ever a signal is encountered, the corresponding access point's power is adjusted until the laptop no longer picks up the signal outside. The result is secure, but has a trade-off. The areas near the outside walls have a weaker signal, reducing the speed the student or teacher can connect to the network. In some zones (libraries, science labs, etc.), two additional access points are installed to account for the higher concentration of users. All access points are powered via Power over Ethernet (PoE) to avoid requiring a power outlet near the access point.

A challenge it faces today in its implementation is that when all the students are in the hallways between classes or on their way outdoors, the wireless signal is negatively affected. This dynamic environmental condition can cause signal drops. It also discovered that with the increase of users on the network required that the backbone switch inter-connects had to be upgraded from 100Mbps to 1 gigabit to handle the traffic loads.

All control and configuration is centralized to head office via SuperNet. This eases management of the networks and provides greater cost savings overall and an increase in control of IT.

Security

From each school, user traffic is routed back through the head office firewall and URL filtering systems to check and log activity for further review and auditing purposes. This solution allows central control and monitoring of students' Internet access. URL and spam filtering is deployed centrally at head office. Random checks are made for user activity that breaks the usage policy code. Immediate action is taken to notify the user of their violation. This has been an effective, low cost technique for Calgary Catholic.

Access points are disabled automatically between the hours of 1am and 6am. Guest access is limited to an 8am to 6pm time window. War driving (the process of driving around with laptops to find wireless networks) is always a concern. All access points are tuned so that their signal does not transmit outside building walls. The Aruba solution automatically disables rogue access points should any be brought into the environment. All wireless laptops must be domain members in order to connect to the wireless network. A group policy object is pushed to the domain members locking their system to the access point's SSID.

Firewalls are deployed throughout the network for network layer protection. All systems run anti-virus software for protection from virus activity. Server certificates are used in authentication ensuring only valid users are associating with the network.

Maintenance and Support

In-house support is covered not only by a head office help desk but by administrators at the school level. Calgary Catholic has 13 school level administrators, 9 at the high schools and 4 setup as roaming administrators that take care of the elementary and junior high schools. Centralization of services and data lowers the complexity of networks and lowers the time required to maintain those systems.

Out-sourcing time consuming work (like hardware warranty work, temporary lab setup and tear down, etc.) saves the in-house IT staff time. The in-house staff can then focus on higher priority functions that keep the network running. When in-house staff is too busy, it will outsource for help.

Students at some of the schools take the laptops home. This often increases the IT support requirements, especially if they are damaged, exposed to high-risk networks or tampered with.

Lifecycle

Calgary Catholic tries to replace its desktop/laptop systems every five years and its server systems every three years. It run this cycle fairly successfully but is still running into funding challenges that can delay the purchase of new hardware.

Conclusion

Calgary Catholic's network is a great example of a well run network of substantial size maintained on a very strict budget by a relatively small team of IT professionals. By purchasing standard hardware from major vendors and maintaining support contracts, it is able to keep support costs at a minimum while gaining access to industry experts.

7.4 Evergreen Catholic School District (ECSD)

Introduction

Evergreen Catholic School Board consists of eight schools. It has implemented a small enterprise wireless network solution at a single school and expects to replace the existing thick access point wireless networks at the remaining seven schools in the near future.

Executive Summary

- *3,320 Students*
- *205 Teachers*
- *8 Schools*
- *6 Wireless Networks*
- *DLink Enterprise Solution. Wireless Switch and Thin APs*
- *3 IT Support Staff*
- *Cost Effective Solution for Smaller School Districts*

Cost Saving Techniques

Several effective techniques were used by Evergreen Catholic to keep costs affordable.

The use of free wireless signal measuring software (Network Stumbler), instead of expensive spectrum analyzers, was used. It chose a functionally comparable but cost effective DLink Enterprise solution for its wireless networks. This solution uses thin access points and is highly affordable for its schools.

Installing Fortinet firewall products instead of higher priced enterprise firewalls was a smart decision.

Evergreen often purchases refurbished computer hardware instead of brand new machines, getting warranty and support contracts on refurbished hardware at a lower cost. The use of spare computers to swap out during level 1 technical support reduces incident resolution time and gets teachers and students back up and productive faster.

Vendor Selection

Evergreen chose DLink Enterprise's wireless network solution for its district. These products are highly affordable and provide the functionality of more established enterprise brand systems.

Implementation

Evergreen approached the rollout of its wireless LAN using floor plans and building specifications to pre-determine the location of its access points. Using the rule of thumb that drywall is easier to go through than cement, it planned its coverage zones. Once it began installation, it used tools such as Net Stumbler (a free software that locates wireless networks and shows signal strengths) to tweak the position of the access points.

Currently, a single school is running a DLink Enterprise thin access point wireless network solution. This will eventually replace the existing thick access point wireless networks currently in place at the other schools. Some of the thick access points do not have RADIUS authentication and are generally lacking modern security. Wireless networks are segmented using VLANs, and traffic between VLANs is firewalled.

Student storage is centralized at the head office for efficiency. With this solution, Evergreen can swap out computers that are at end of their life span, increasing technical support efficiency.

Security

A deployment of Fortinet firewalls protect and connect the Evergreen Catholic schools with district head office and the Internet. It uses the content filtering features of these units to protect its users from dangerous content and give each school the ability to white and black list URLs. All schools are connected via a virtual private network to head office.

Inter VLAN traffic is firewalled and all wireless networks are isolated for security. Evergreen has noticed students bringing in USB memory sticks and with installed software on them. These pose a risk to the internal network should it contain viruses or other malicious programs. There is no compliance software solution in place. Students bringing home laptops often introduce security threats when they re-connect to the school LAN. This is very challenging to manually control in an ad-hoc fashion for any IT staff.

Maintenance and Support

Evergreen IT staff makes heavy use of BlackBerries while providing support to schools. All communication is work order driven and is tracked and managed electronically. Support is allocated to schools based on their student populations. A Windows Software Update Services server is used to manage the security patches on its desktop machines. All servers and access points online status is monitored continuously. Support is delivered via Remote Desktop connections over the VPN.

Students and teachers are not very technically savvy and are struggling with the technology to some degree. Over time, this will improve, but initially, there is a heavy burden on IT staff to help and train users.

For every 30 students, Evergreen has 34 computers. This allows for simple swapping of a system if it begins to malfunction. This is a very good level 1 strategy to optimize a small IT team's time, allowing it to physically get to any individual school site and perform system restores in a more scheduled manner.

Lifecycle

There is no official policy on the life cycle of the hardware that Evergreen uses. The typical trend is to use hardware until it begins to malfunction and the IT staff identifies a particular client or device as end of life.

Conclusion

The Evergreen IT infrastructure is the result of a small board making good decision on what product and vendors to work with. The solutions from Fortinet and DLink are very cost effective for the functionality gained from them makes its WLAN and WAN manageable in a cost effective manner.

AES	Advanced Encryption Standard
AP	Access Point. A generic description given to a network access device. It may be a wireless router.
BSS	Basic Service Set. Describes a wireless network with a permanent installation where one of the devices (an AP) forwards the frames between stations as well as between the stations and a Wired Network.
BSSID	Basic Service Set Identifier. Not to be confused with SSID. In an infrastructure network or BSS, this is the MAC address of the AP. In an IBSS, this will be a random number in the form of a MAC address. However, due to the ability of the clients to join and leave the IBSS, this ID can stay with the network as long as it is operational.
CA	Collision Avoidance
CSMA	Carrier Sense Multiple Access
DSSS	Direct Sequence Spread Spectrum. A technology that uses more bandwidth than is actually required to transmit the signal. It achieves this by taking the information "bits" and representing each bit with a predetermined string of 1's and 0's. While this may seem like a waste it creates a signal that is resilient to interference and allows it to be transmitted at very low power values.
ESS	Extended Service Set. Describes a wireless with multiple APs sharing a common SSID. This allows clients to roam between APs while maintaining a network connection.
FHSS	Frequency Hopping Spread Spectrum. A technology that uses frequency agility to spread data over a wide portion of the spectrum. The main items are how long the radios stay on a channel, how many channels are in its hop pattern, and how fast it can "hop" to another channel.
IBSS	Independent Basic Service Set. Describes a wireless network that is made up on client devices only. It allows short-term ad-hoc connections and it often referred to as an ad-hoc or peer-peer network.
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IEEE	Institute Of Electronic And Electrical Engineers
IP-PBX	IP-Private Branch Exchange
IPS	Intrusion Prevention System
MIMO	Multiple Input, Multiple Output
MSP	Mobile Services Platform
NAC	Network Admission Control. Describes is a set of technologies and solutions designed specifically to help ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats.
OFDM	Orthogonal Frequency Division Multiplexing. OFDM is a technology that is <i>spread spectrum like</i> , although it is not a true spread spectrum technology. It takes information and multiplexes it onto a group of carefully planned out sub-carriers. Each sub-carrier has a relatively low data rate, but by transmitting data in parallel on these sub-carriers, it creates the highest throughput of any current technology.
QOS	Quality Of Service
RF	Radio Frequency
SMB	Small And Midsize Business
SOHO	Small Office/Home Office
SSID	Service Set Identifier. Describes a particular network, comprising of 2 - 32 unique case sensitive ASCII characters.
VoIP	Voice Over IP
VoWLAN	Voice Over WLAN
VPN	Virtual Private Network

WCS	Wireless Control System
WEP	Wired Equivalent Privacy
WEP	Wired Equivalent Privacy. The initial layer 2 method of encrypting data over a wireless link. It requires the entry of a static key on all network devices.
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access. This is a certification released by the Wi-Fi alliance to provide improved security during the time that 802.11i was being developed. It defines advanced modes of authentication and encryption as well as being backwards compatible with WEP.
WPA2	Wi-Fi Protected Access 2
WPA2/802.11i	WPA2 is the certification released by the Wi-Fi Alliance which is based on the completed 802.11i standard.

Resources and Sources

Links

- www.ieee.org
- www.nist.gov
- <http://www.cisco.com/go/unifiedwireless>
- http://www.cisco.com/en/US/products/hw/wireless/products_category_buyers_guide.html
- <http://www.hp.com/rnd/pdfs/802.11technicalbrief.pdf>
- http://www.hp.com/rnd/pdf_html/wirelessLANsite_assessment.htm
- http://www.hp.com/rnd/pdfs/antenna_tech_brief.pdf
- http://www.hp.com/rnd/pdfs/Mobility_Infrastructure_Tech_Brief.pdf
- http://www.hp.com/rnd/pdfs/Mobility_Infrastructure_Solutions_Brochure.pdf
- http://www.hp.ca/govonline/provincial/pricing/hp_pscustomer.xls
- www.symantec.com
- www.8e6.com
- www.fortinet.com
- www.checkpoint.com
- www.barracudanetworks.com
- www.surfcontrol.com
- www.flukenetworks.com/wireless
- www.airmagnet.com/products/laptop.htm
- www.wildpackets.com/products/omni/overview/omnipeek_analyzers
- www.airmagnet.com
- www.netstumbler.com
- <http://www.tek.com/products/communications/products/wireless/index.html>
- www.cognio.com